
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# ZAVÁDĚNÍ ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI VE ZDRAVOTNICKÉM ZAŘÍZENÍ

THE IMPLEMENTATION OF INFORMATION SECURITY IN HEALTHCARE ORGANIZATION

**DIPLOMOVÁ PRÁCE**
MASTER'S THESIS


**AUTOR PRÁCE** — **Bc. Lucie Procingerová**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Petr Sedlák**
SUPERVISOR



**BRNO 2017**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Studentka: | **Bc. Lucie Procingerová** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Informační management |
| Vedoucí práce: | **Ing. Petr Sedlák** |
| Akademický rok: | 2016/17 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

## Zavádění řízení informační bezpečnosti ve zdravotnickém zařízení

**Charakteristika problematiky úkolu:**

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Pro vybrané zdravotnické zařízení na základě analýzy vypracujte metodický postup pro zavedení ISMS.

**Základní literární prameny:**

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

L. S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

## Abstrakt

Předkládaná diplomová práce vychází z poznatků informační bezpečnosti a jejího řízení. Práce je členěna do dvou částí. První část poskytuje teoretická východiska, definice a terminologii v souvislosti s řízením informační bezpečnosti a opírá se také o pojmy z ISO norem řady 27000. Druhá část se zabývá analýzou vybrané společnosti. V návaznosti na tuto analýzu je vypracován návrh na zavedení systému řízení informační bezpečnosti (ISMS) do podniku a bezpečnostní příručka. Tato příručka obsahuje nejen doporučení pro řízení bezpečnosti v ICT, ale i rady v oblasti personální či fyzické bezpečnosti podniku.



## Abstract

This Master‘s thesis is based on knowledge of information security and its management. The thesis is divided into two parts. The first part provides the theoretical background, definitions and terminology according to the information security management and it is based on concepts from standard ISO 27000 series. The second part aims to analysis of a selected company. Following to this analysis proposal of implementation of information security management system and security guide is drawn up. This guide contains recommendations for ICT security management and advices in field of personal and physical security in company.



## Klíčová slova

ISMS, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, ČSN ISO/IEC 27799, zdravotnictví, bezpečnost, management bezpečnosti, zdravotnická bezpečnost

## Keywords

ISMS, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, ČSN ISO/IEC 27799, healthcare, security, security management, health security

## Bibliografická citace

PROCINGEROVÁ, L. *Zavádění řízení informační bezpečnosti ve zdravotnickém zařízení.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 99 str. Vedoucí diplomové práce Ing. Petr Sedlák.

# Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Dále prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 26. května 2017

……...

Lucie Procingerová

## Poděkování

Ráda bych poděkovala panu Ing. Petru Sedlákovi za nespočet rad při tvorbě této práce a ze trpělivé vedení, které mi poskytl. Dále bych ráda poděkovala svojí rodině a přátelům bez jejichž trpělivost a shovívavosti by nemohla práce vzniknout.

# Obsah

# 1 Úvod

V současné době, kdy jsou informační a komunikační technologie naprosto nezbytné pro fungování téměř každé moderní společnosti, stoupá také riziko zneužití těchto systémů. Lidé je využívají ve svém každodenním životě – v práci, doma, při nákupu, při styku s veřejnosprávními orgány atd. Společnosti vlastnící tyto systémy je využívají jako konkurenční výhodu. Výhoda se dá chápat ve dvou rovinách. První výhodou může být, že daný systém vůbec vlastní a umí si s ním zjednodušit a zefektivnit pracovní činnosti. Druhá rovina může být chápána jako schopnost s těmito systémy správně zacházet. To obnáší nejen standardní obsluhu komunikačních a IT zařízení, ale i uvažování nad bezpečným používáním. Správností využití informačních technologií, tedy umění zacházet s daty a také jak je správně chránit, se budu zabývat v této diplomové práci.

Většina společností je zcela závislá na využití služeb informačních a komunikačních technologií. Jakékoliv narušení by mohlo znamenat ztráty, a dokonce může ohrozit fungování podniku. Často jsou systémy tak úzce propojené, že i malé zakolísání jednoho prvku ovlivní celý systém. I menší chyby či krátkodobá nedostupnost systému může nést velké důsledky. Proto se v této souvislosti stále častěji objevuje pojem management informační bezpečnosti. Jestliže ztráta některé informace nebo dat představuje pro společnost vážnou hrozbu, je vhodné nad informační bezpečností uvažovat.

Ve zdravotnictví, kde je kompromitace citlivých údajů obzvláště závažná, se problematika bezpečnosti v České republice stále zanedbává. Mnohokrát totiž lékař nemá čas na zajištění ochrany dat. Leckdy ani nemá takový rozhled v oblasti, která se neustále vyvíjí, a to velmi rychlým tempem. Nutno však myslet na to, že bezpečnost je hlavně o lidech a jejich řízení. Bezpečnost není jen hardware a software. Ale zejména lidé, kteří s těmito zařízeními pracují a využívají je, resp. zneužívají ve prospěch či neprospěch celého systému. Často se také zapomíná na běžného uživatele, který má ve zvyku si věci ulehčovat, obcházet stanovená pravidla, jednat impulzivně a v neposlední řadě mýlit se.

Oblast ochrany informací je velmi široká a není úplně jednoduché ji zabezpečit komplexně. Ohrožení informací může nastat také fyzickým napadením, neoprávněným přístupem nebo špatnou manipulací.

Tato diplomová práce se zabývá řešením bezpečnosti informací ve zdravotnictví a je zde vysvětleno, jak bezpečnost zajistit. Práce může sloužit také jako referenční materiál pro přípravu na certifikaci dle ISO normy 27001 nebo i jako příprava na nařízení Evropského parlamentu o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, které nabude platnost v květnu 2018.

Celý dokument je rozdělen na dva hlavní segmenty. V první části jsou nastíněna teoretická východiska, jenž slouží jako podklad pro část druhou. Teorie obsahuje popis a vysvětlení pojmů, zákonů a norem. Druhá část se již zabývá konkrétním řešením pro danou společnost. V této části lze nalézt informace o společnosti. Následuje analýza, abychom měli představu, co již společnost vlastní a využívá za IT zařízení a jak se doposud ochranou informací zabývá. V návaznosti na tuto analýzu je vytvořena bezpečnostní příručka, která obsahuje doporučení, rady a postupy pro zajištění bezpečnosti informací. V závěru se pak nachází shrnutí a zhodnocení.

# 2 Vymezení problému a cíle práce

Stále častěji lze ve zprávách zaslechnout, že byla ohrožena data některé nemocnice nebo kliniky. V nemálo případech už také došlo ke ztrátám těchto dat a zdravotnická zařízení pak mají problémy se špatnou pověstí, což může vést k nedůvěře ze strany veřejnosti. Evropská policejní agentura Europol dokonce zaznamenala přímo ve zdravotnictví[1] pokusy o počítačové vydírání prostřednictvím programů únosců, kterým se odborně říká malware. Ohrožení se ale nemusí týkat jen nemocnic či ordinací. Známé jsou útoky i na zdravotní pojišťovny. Příkladem může být článek zveřejněný dne 5. února 2015 na serveru Lidovky.cz, kde je popsáno následující, cituji:

*„Druhá největší americká zdravotní pojišťovna Anthem se stala terčem útoku hackerů, kteří ukradli osobní informace o jejích současných i bývalých klientech z databáze zahrnující zhruba 80 milionů lidí. Mezi ukradenými informacemi jsou například údaje o příjmech či adresy.“*[2]

Dalším důvodem pro zavedení ISMS je plánovaná elektronizace zdravotnictví, tzv. eHealth. Zavedení plánují instituce České národní fórum pro eHealth a ICT Unie pod záštitou Ministerstva zdravotnictví. V konceptu eHealth lze nalézt seznam oblastí, kterých se elektronizace týká. Jsou to například zdravotnické dokumentace, identifikace pacientů a zdravotníků nebo také vzdělávání pro občany i zdravotnický personál.[3]

Nové nařízení Evropské unie o ochraně a zpracování osobních údajů může být důvodem třetím. Toto nařízení má anglický název General Data Protection Regulation (GDPR) a přináší dosud největší revoluci v této oblasti. Zajímavé až odstrašující jsou stanovené výše pokut, které při porušování mohou dosáhnout až na 20.000.000 eur. V České republice toto obecné nařízení nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních

[1] Zdroj: http://zpravy.idnes.cz/pocitacova-kriminalita-europol-terorismus-fe6-/zahranicni.aspx?c=A160928_102420_zahranicni_pku
[2] Zdroj: http://byznys.lidovky.cz/hackeri-zautocili-na-velkou-pojistovnu-v-usa-ukradli-adresy-klientu-1i5-/firmy-trhy.aspx?c=A150205_090532_firmy-trhy_ele
[3] Zdroj: http://www.ezdrav.cz/ehealth-v-cr/

údajů.[4] S problematikou úzce souvisí také zákon č. 181/2014 Sb. o kybernetické bezpečnosti.

Všechny výše vypsané důvody by měly vést zdravotnické organizace ke zlepšení stavu jejich bezpečnosti a k lepší ochraně shromažďovaných dat.

Cíle této práce lze shrnout do dvou hlavních bodů:

1. Popsat a zaznamenat problematiku zavádění ISMS do zdravotnictví v souladu s normou ČSN ISO/IEC 27799:2010.
2. Vytvořit bezpečnostní příručku na základě analýzy vybrané společnosti, která bude sloužit jako dokument pro nasazení ISMS do praxe.

[4] Zdroj: https://www.gdpr.cz/

# 3 Teoretická východiska

V této kapitole rozeberu teorii potřebnou k praktické části. Jedná se zejména o vysvětlení několika pojmů z informační bezpečnosti, vysvětlení ISMS od zavedení až po údržbu, pojmy ze zdravotnictví a bezpečnost řešená ve zdravotnictví. Zabývat se budu i legislativním prostředím v České republice, tj. normami, zákony a nařízeními.

V knize o řízení bezpečnosti informací (1), jsem nalezla související motto:

*„Bezpečnost je tak účinná, jak je silný její nejslabší článek."*

## 3.1 Základní pojmy informační bezpečnosti

Na úvod této práce je zcela nezbytné vysvětlit několik pojmů z bezpečnosti, které se zde budou častěji opakovat.

Nejčastější termíny, které jsou také několikrát zmíněny v ISO[5] normách řady 27000:

**Bezpečnost informací** (Information Security) – znamená zachování důvěrnosti, integrity a dostupnosti informací. Velmi úzce souvisí s bezpečností organizace a IS/ICT. Bezpečnost organizace je nadřazena bezpečnosti informací.

**Důvěrnost** (Confidentality) – zajištění přístupu k informacím pouze oprávněným osobám.

**Integrita** (Integrity) – zajištění správnosti a úplnosti informací.

**Dostupnost** (Availability) – zajištění přístupnosti k informaci oprávněnému uživateli v požadovaný okamžik.

**Aktivum** (Asset) – veškerý hmotný a nehmotný majetek.

**Hrozba** (Threat) – potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.

**Zranitelnost** (Vulnerability) – slabé místo aktiva.

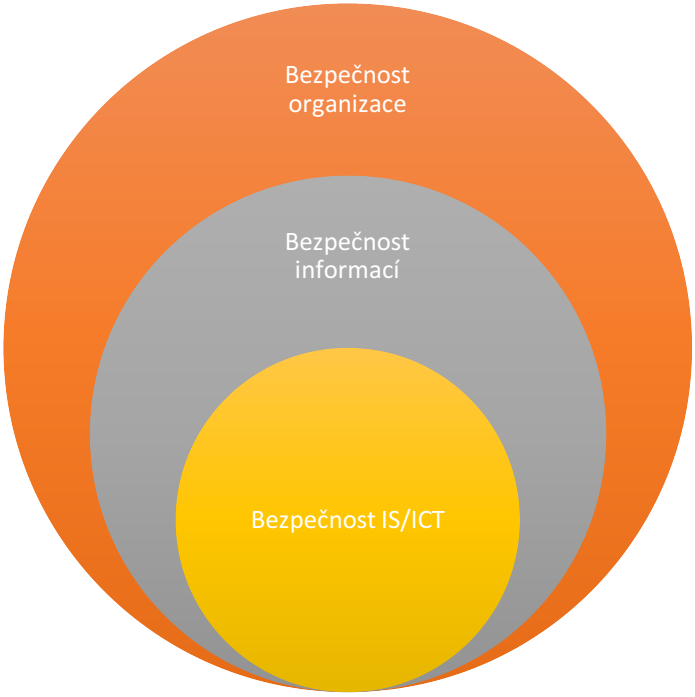
**Riziko** (Risk) – kombinace hrozby a zranitelnosti s dopadem na aktivum.

[5] ISO (International Organisation for Standardisation)

**Bezpečnostní událost** (Information Security Event) – zjištěný výskyt stavu systému, služby nebo sítě označující možné narušení politiky bezpečnosti informací nebo selhání bezpečnostních opatření.

**Bezpečnostní incident** (Information Security Incident) – nestandardní a nežádoucí bezpečnostní událost, která vede k narušení pravidel bezpečnosti informací.

**Shoda** (Conformity) – splnění požadavku.




Obrázek 1: Vzájemné vztahy bezpečnosti v organizaci, zdroj: vlastní tvorba dle (2)

Převzato ze zdrojů (2) a (3).

## 3.2 Systém řízení informační bezpečnosti (ISMS)

Název pochází z anglického překladu Information Security Management System. A jak samotné slovní spojení napovídá, jedná se o řízení bezpečnosti z pohledu informatiky a managementu. Důležité je uvědomit si, že ISMS patří do celkového systému řízení organizace.

### 3.2.1 Demingův cyklus

Demingův cyklus (nebo také PDCA cyklus) je metoda postupného zlepšování. Může se jednat o zkvalitňování služeb, procesů nebo čehokoliv dalšího. Zkratka PDCA vychází z anglických termínů – Plan (plánuj), Do (dělej), Check (kontroluj) a Act (jednej). Tento model byl poprvé použit americkým statistikem W. E. Demingem v souvislosti s inovací a nasazováním systému řízení do průmyslu. V současnosti je ale využíván jako základ mezinárodních standardů, včetně oblasti řízení bezpečnosti informací (1).

Čtyři etapy, které se opakují (2):

- **P**lan – naplánování zamýšleného zlepšení,
- **D**o – realizace plánu,
- **C**heck – ověření výsledku realizace oproti původnímu záměru,
- **A**ct – úpravy záměru i vlastního provedení na základě ověření a plošná implementace do praxe.

Součástí modelu PDCA je i dokumentace každé jeho etapy, jenž je často vnímána jako nejméně příjemná část. Avšak dokumentace je klíčová.

Důležité je dodržovat i zásady procesního řízení. Procesy je třeba:

- identifikovat,
- popsat a zdokumentovat,
- na základě dokumentace procesy řídit,
- optimalizovat jejich průběh.


Obrázek 2: Princip Demingova modelu PDCA v ISMS, zdroj: vlastní tvorba dle (2)

Z výše uvedeného obrázku lze rozpoznat, že ISMS přesně využívá definovaný model a z toho také vychází čtyři etapy (1):

- Ustanovení ISMS – tato etapa si klade za cíl upřesnění rozsahu a hranic, kterých se bude řízení bezpečnosti týkat, dále stanovuje jasné manažerské zadání a vybírá opatření na základě analýzy rizik.
- Zavádění a provoz ISMS – zde je cílem účelně a systematicky prosadit v přechozí etapě stanovená opatření do chodu organizace.
- Monitorování a přezkoumání ISMS – v této etapě je hlavním cílem zajištění zpětné vazby, pravidelného sledování a ohodnocení úspěšných, ale i nedostatečných stránek řízení bezpečnosti informací.
- Údržba a zlepšování ISMS – v poslední etapě je cílem realizace dalších možností zlepšování systému řízení bezpečnosti informací, a to buď soustavným zlepšováním systému, nebo odstraňováním zjištěných chyb a nedostatků.

Následující popis jednotlivých etap je převzat ze zdroje (1).

**Ustanovení ISMS**

Tato etapa budování má zásadní dopady na fungování ISMS během jeho celého životního cyklu. Kromě toho, že se v této fázi stanovují rozsahy ISMS, je nutné mít odsouhlasený také dokument „Prohlášení o politice ISMS“, ve kterém lze nalézt potvrzený závazek od managementu podniku k podporování informační bezpečnosti. Další činností je provedení analýzy rizik a v návaznosti na tuto analýzu se stanovují také vhodná bezpečnostní opatření pro snížení vlivu nalezených bezpečnostních rizik. Etapa se ukončuje souhlasem vedení se zavedením ISMS dle potřeb organizace, zjištěných při analýze a zvládání rizik ISMS.

**Zavádění a provoz ISMS**

Tento úsek navazuje na navržená opatření z předchozí etapy. Soustředění je zacíleno na prosazení všech bezpečnostních opatření. Připravují se dílčí plány s přesně stanovenými termíny, seznamem odpovědných osob atd. Všechna bezpečnostní opatření jsou pak shrnuta v dokumentu zvaném „Příručka bezpečnosti informací“. V tomto stádiu je také důležité nezanedbat proškolení všech uživatelů.

**Monitorování a přezkoumání ISMS**

V této etapě je důležitým úkolem zajištění účinné zpětné vazby. V souvislosti s tím by mělo dojít k prověření všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Ověření provádí přímý nadřízený nebo bezpečnostní manažer na pověřených a odpovědných osobách. Pomocí interních auditů lze také nezávisle posoudit fungování účinnosti ISMS. Všechny použité zpětné vazby by měly přinést co nejvíce kvalitních podkladů o skutečném fungování ISMS. Tyto podklady se poté předávají vedení, které rozhodne, zda je realizace ISMS v souladu s obecnými potřebami organizace.

**Údržba a zlepšování ISMS**

V poslední fázi by mělo docházet ke sběru podnětů na zlepšení a k nápravě všech nedostatků, tzv. neshod, které se v ISMS objevují.

Po zavedení ISMS do společnosti je možné spatřovat několik výhod (1):

- zlepšení procesů v organizaci, vyšší účinnost a účelnost,
- konkurenční výhodu,
- záruku zajištěné bezpečnosti informací a také ochrana dat jiných subjektů, jejichž data jsou zpracovávána,
- nižší míru rizika související s nedostupností služeb, únikem nebo ztrátou dat,
- optimalizaci výdajů v souvislosti bezpečností a identifikovanými aktivy,
- méně časté odstraňování následků bezpečnostních incidentů a tím i větší úsporu nákladů,
- lepší přípravu organizace na obnovení chodu po výpadku informačního systému (tím se optimalizují výdaje na tuto obnovu),
- zlepšení image firmy před klienty, partnery, nadřízenými orgány, orgány státní správy i před veřejností,
- důkladnější proškolení pracovníků a dalších uživatelů,
- větší pořádek na pracovišti,
- vypracování havarijních plánů pro případ ohrožení.

## 3.3 Postup zavedení IT bezpečnosti

Při budování systému řízení bezpečnosti informací je nezbytné realizovat celý životní cyklus ISMS, jehož definici nalezneme v ISO/IEC 27001:2014. Zejména nezbytný je tento postup, pokud chce daná společnost dosáhnout na certifikaci. Nicméně i v případě nižších ambicí lze tento proces doporučit a není na škodu se ho držet.

Aby byl ISMS správně zaveden, je zde seznam klíčových činností, které je třeba dodržovat (4):

- Působnost ISMS – na základě cílů a strategie organizace se určuje, které části organizace budou do ISMS zahrnuty.

- Prohlášení o politice ISMS – tento dokument má za úkol stanovit celkový směr realizace ISMS, určují se zde cíle a strategie ISMS, vymezují se požadavky na ISMS (např. legislativní požadavky, smluvní závazky organizace). Určují se také kritéria pro hodnocení rizik.
- Analýza a zvládání rizik – na základě rozboru se určují a vybírají všechna bezpečnostní opatření, jejich účinnost a účelnost. Nevyžadují se zde žádné speciální techniky, nicméně je tato analýza stěžejní krok.
- Prohlášení o aplikovatelnosti – v dokumentu jsou upřesněna bezpečnostní opatření, která se budou aplikovat. Zde je velmi důležité, aby management společnosti uvážil a pečlivě vybral ta opatření, která mají optimální náročnost z hlediska personálního i finančního.
- Plán zvládání rizik – dokument jasně vymezuje stanovené odpovědnosti, činnosti a priority pro řízení rizik bezpečnosti informací.
- Záznamy[6] – tvoří hlavní prvek systému řízení, jímž se prokazuje i jeho správné fungování.
- Přehodnocení – pravidelně opakující se úkon, při kterém se výsledky ISMS prezentují vedení společnosti. Cílem je seznámení vedení o stavu ISMS, upřesnění plánu a nadefinování následujícího postupu (zpravidla na jeden rok dopředu).

Normy nám pomáhají zajistit bezpečnost po stránce řízení. Informační bezpečnost se dá rozdělit na několik druhů (5):

- Fyzická bezpečnost – zahrnuje hlavně ochranu proti neoprávněnému vniknutí osob, způsoby zničení informací na záznamových médiích (CD, DVD, tištěné materiály) a také ochranu proti přírodní živlům.
- Počítačová bezpečnost – zahrnuje výběr a spolehlivost technických prostředků, zabezpečení jejich okamžitého servisu a kontrolu přístupu k těmto prostředkům.
- Personální bezpečnost – zabývá se hlavně eliminací hrozeb způsobených lidským faktorem. Zahrnuje ochranu zaměstnanců a ochranu technického vybavení před nesprávným použitím. Definuje pravomoci a zodpovědnosti pracovníků i zaměstnanců třetích stran.

[6] Záznam je doklad o tom, že byla provedena určitá činnost včetně informací o obsahu a výsledku dané činnosti.

- Komunikační bezpečnost – zabývá se ochranou dat v souborech/databázích proti odposlouchávání/modifikování při jejich přenosu, ochranou proti škodlivým kódům a ochranou před neoprávněným průnikem z internetové sítě.
- Logická bezpečnost – zabývá se zabezpečením kontroly přístupu, identifikací a autentizací uživatelů, rozdělením pravomocí uživatelům, sledováním a záznamem činností systému a uživatelů. Patří sem i výběr a spolehlivost programového vybavení, jeho licenční čistota a kontrola k jeho přístupu.

### 3.3.1 Obsah ISMS a jeho etapy

ISMS pomáhá eliminovat ztrátu nebo poškození informačních aktiv pomocí několika bodů:

- jsou přesně stanovená aktiva, která se mají chránit,
- zjištěná rizika jsou řízena,
- jsou nastavena opatření pro snížení definovaných rizik a jsou kontrolována.

ISMS je možné zavést do jakékoliv organizace. Může zasahovat plošně do všech oddělení. Ale zároveň je ho možné implementovat pouze do některých částí organizace či jen na určitou pobočku. Rozhodnutí o rozsahu má plně v moci management společnosti.

Následující text se opírá o zdroj (2).

ISMS zahrnuje tyto základní okruhy:

- IT bezpečnost,
- komunikační bezpečnost,
- personální bezpečnost,
- administrativní bezpečnost,
- fyzická bezpečnost,
- dokumentace,
- bezpečnostní funkce a mechanizmy.


Obrázek 3: Oblasti ISMS dle přílohy a normy ČSN ISO/IEC 27001:2014, zdroj: vlastní tvorba

Zavedení do ISMS nemusí nutně končit jeho certifikací. Je ho možné zavést i bez ní. Pokud však společnost chce certifikace dosáhnout, měla by projít několika etapami. Právě **odsouhlasení managementu** k zavedení je první dokument, který auditoři požadují, má-li se systém řízení bezpečnosti certifikovat. Dokument nemusí být rozsáhlý, ale musí v něm být obsažen jasný souhlas od vedení a zároveň také prokázána shovívavost při zavádění. To znamená, že společnost věnuje pro zavedení minimálně lidské zdroje a finance.

Ve druhé fázi se již vše zaměřuje na **aktiva, jejich ohodnocení** a následně i vypracování **analýzy rizik**. Aktiva se musí nejprve identifikovat a pak ocenit. V potaz se berou hmotná

i nehmotná aktiva. Ohodnocení je postaveno na základě společností vyspecifikovaného algoritmu, který určí jejich hodnotu v souvislosti s důvěrností, integritou a dostupností. Druhá část této fáze je analýza rizik. Ta se opět provádí pomocí vybrané metodiky. Tento dokument je stěžejní část a musí být velmi dobře vypracován. Na dokumentu totiž stojí celý systém bezpečnosti informací.

Třetí etapa navazuje na analýzu rizik a zpracovává se v ní další potřebný dokument. Nese název ***Návrh opatření.*** Je v něm obsažen soupis všech bezpečnostních opatření, které jsou spojena s nalezenými riziky. Opatření se navrhují taková, aby byla schopna rizika eliminovat. V tomto úseku se vytváří ještě další dokument. Obsahuje cíle opatření a definice všech bezpečnostních opatření, která jsou relevantní a aplikovatelná. Dokument se nazývá ***Prohlášení o aplikovatelnosti***.

V poslední etapě je pak na zvážení společnosti, zda si celý systém nechá nebo nenechá rovnou certifikovat. Certifikace není nutná a skládá se ze dvou částí. Nejdříve se certifikuje povinná dokumentace, následně probíhá kontrola praktického zavádění ISMS.

Veškerá činnost, provedené procesy a rozhodnutí vedení se musí dokumentovat, aby bylo možné všechno zpětně dohledat. Jedná se celkem o 11 dokumentů.

1. Rozsah a hranice ISMS – jasně stanovuje, kterých částí organizace se ISMS bude týkat. Dokument se vypracovává na základě posouzení různých rysů organizace.
2. Politika ISMS – v dokumentu se vedení společnosti zavazuje k tomu, že chápe veškeré souvislosti spojené s ISMS. Také že nejen při zavádění, ale i do budoucna, bude poskytovat personální, technické a finanční zajištění.
3. Definice a popis k přístupu hodnocení rizik – stanovuje použitou metodu pro nalezení a hodnocení rizik.
4. Identifikace a ohodnocení aktiv – ve formě slovního popisu a přehledné tabulky se zde vyjmenují všechna aktiva, jejich majitelé a ohodnocení. Definuje také metodu použitou pro hodnocení aktiv.
5. Identifikace rizik – někdy bývá součástí předešlého dokumentu. Jsou zde popsány konkrétní výsledky hodnocení rizik, obsahuje název informačního systému a odkazuje na metodiku, která byla použita pro hodnocení rizik. Obsahem bývá i tabulka s možnými hrozbami a mírou rizika.

6. Analýza rizik – popisuje principy analýzy rizik, aktiva, rizika a výsledky analýzy rizik.
7. Návrh opatření – objasňuje minimalizaci zjištěných rizik. Může se zde objevit konkrétní i obecný návrh řešení. V dokumentu jsou popsána i akceptovatelná rizika.
8. Cíle opatření a bezpečnostní opatření pro zvládání rizik – dokument vychází z přílohy obsažené v normě ISO/IEC 27001. V příloze nalezneme definice cílů opatření a jednotlivých bezpečnostních opatření, jež jsou použitelná pro různé typy organizací.
9. Akceptace rizik – vychází z dokumentu návrhů opatření. Akceptaci rizika provádíme tehdy, kdy je nápravné opatření extrémně drahé a míra rizika je velmi nízká. V tomto dokumentu jsou akceptovaná rizika vypsána a schválena nebo zamítnuta.
10. Získání povolení k provozování ISMS v rámci organizace – v tomto dokumentu se vedení společnosti zavazuje k ustavení, zavedení, provozu, monitorování, přezkoumání, udržování a zlepšování ISMS.
11. Prohlášení o aplikovatelnosti – jsou zde popsány cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS. Dokument také poskytuje ucelený souhrn rozhodnutí, jakým způsobem bude nakládáno s identifikovanými riziky.

### 3.3.2 Personální a administrativní bezpečnost

Tato oblast nezahrnuje pouze interní zaměstnance organizace, ale komplexně řízení lidských zdrojů. Jedná se tedy i o pracovníky smluvních stran a celý životní cyklus interních zaměstnanců (1). V normě ISO/IEC 27001 je v příloze uvedená tabulka *Cíle opatření a jednotlivá opatření*, kde pod označením A.7 nalezneme právě onu bezpečnost lidských zdrojů. Ta je rozdělena na tři podkategorie (6):

- před vznikem pracovního vztahu,
- během pracovního vztahu,
- ukončení a změna pracovního vztahu.

Oblast bezpečnosti lidských zdrojů by se měla promítnout do všech firemních procesů, směrnic a nařízení. Zaměstnanci (i např. brigádníkovi) se zřizuje e-mailový účet, přiděluje heslo, dostane svůj pracovní počítač. Postupem v kariéře tak může dostávat nová oprávnění (7).

Při nástupu je potřeba připravit počítač se správným nakonfigurováním, zaměstnanec musí být proškolen a seznámen s bezpečnostními směrnicemi. Vyžaduje-li zaměstnavatel speciální prověření (např. určitý stupeň utajení) musí se podepsat dokument o mlčenlivosti nebo použít k prověření nezávislou autoritu.

V průběhu běžného života zaměstnance často není třeba cokoliv měnit. Situace ale může některé úpravy požadovat zejména při změně pracovní pozice. Nové oprávnění by mělo řešit IT oddělení spolu s personálním. O přístupy by neměl zaměstnanec žádat sám.

Při rozvázání pracovního poměru je třeba rozlišovat:

- přátelský odchod,
- nepřátelský odchod,
- odchod ke konkurenci.

Problém by mohl nastat u nepřátelského odchodu, kdy se zaměstnanec může chtít pomstít. Pokud byl najat konkurencí, mohl by informace nabyté v přechozí práci zneužít a vyzradit cokoliv. Proto je velmi důležité, aby se po jeho odchodu znemožnilo použít přístupová hesla, která měl přidělena, měla by se zrušit e-mailová adresa, přeinstalovat počítač apod.

Školení bylo již zmíněno v souvislosti s nástupem nového zaměstnance. Je ale důležité proškolovat personál i v průběhu pracovního poměru. Přímo v normě ISO 27001 je uvedeno v bodě A.7.2.2., že všichni zaměstnanci (potažmo i smluvní strany) musí na základě svého pracovního zařazení dostat odpovídající a opakující se školení (6).

### 3.3.3 Měření účinnosti, monitorování a audity

K prosazení efektivního řízení bezpečnosti patří i měření účinnosti. Měření je proces získávání informací o účinnosti ISMS a bezpečnostních opatření. O měření a bezpečnostních technikách se lze dočíst v normě ISO/IEC 27004.

Pravidelně je třeba také přezkoumávat účinnost navržených bezpečnostních opatření. V potaz se berou výsledky bezpečnostních auditů, incidentů, výsledky měření účinnosti opatření i návrhy a podněty zainteresovaných stran. Všechny tyto činnosti patří pod poslední krok celého cyklu prosazování ISMS – údržba a zlepšování (2).

### 3.3.4 Bezpečnostní projekt

**Bezpečnostní strategie** – jsou v ní definovány základní principy bezpečnostní politiky. Strategie je zcela nezávislá na používaném technickém vybavení nebo personálních funkcích. V tomto dokumentu je stanoven rozsah chráněných informací, důvod jejich ochrany a určení zodpovědností. Dokument musí být obecný a je třeba s ním seznámit všechny zaměstnance. Jedná se o zpracování metod, principů a opatření do detailní podoby. Každá část bezpečnostního procesu má svůj vstup a výstup (8).

**Bezpečnostní projekt** – praktická implementace bezpečnostní politiky v organizaci (2).

Vstupy pro zpracování bezpečnostních projektů:

- strategická bezpečnostní politika,
- požadavky bezpečnostního managementu,
- požadavky a návrhy řešení bezpečnostních konzultantů,
- požadavky od vedoucích pracovníků.

Výstupy bezpečnostního projektu:

- organizační a administrativní opatření (dokumentace a krizové plány),
- technická a technologická opatření (HW, SW, pracovní postupy atd.).

Další výstupní návazné dokumenty jsou různé podnikové směrnice (funkční bezpečnostní politika IS, personální bezpečnostní politika IS, řešení bezpečnostních incidentů, …), metodiky (metodika vývoje IS, zavádění IS do provozu, …) a provozní řády (provozní řády oddělení, aplikací).

### 3.3.5 Analýza rizik

Analýza rizik je prováděna za účelem identifikace zranitelných míst informačního systému organizace.

**Aktiva**

Aktiva je třeba definovat a klasifikovat, následuje jejich hodnocení vybranou metodou a výpočet hodnoty aktiva.

Dle přílohy normy ISO/IEC 27001 musí být vytvořený seznam aktiv neustále aktuální, konzistentní a přesný. Každé aktivum má určeno vlastníka. Musí být jasně dáno, jak s příslušnými informacemi a aktivy zacházet. Případně při rozvázání pracovního poměru, musí zaměstnanec svěřená aktiva vrátit (6).

Aktiva ISMS lze rozdělit do dvou skupin (1):

1. Primární aktiva (nehmotná aktiva) – patří sem: informace, které jsou organizací využívány, funkční procesy a aktivity organizace, znalosti a know-how (významná pro ISMS).
2. Sekundární aktiva (hmotná aktiva) – patří sem: technické vybavení, komunikační infrastruktura, programové vybavení, zaměstnanci, prostory.

Pro každé aktivum se stanovuje míra jeho důvěrnosti, integrity a dostupnosti. Dále je vhodné si aktiva seřadit do skupin s ohledem na jejich hodnocení. Usnadní to pak následné hodnocení a zvládání rizik.

Hodnocení aktiv je možné dělat ve specializovaných programech[7] nebo například v MS Excel. Dále je nutné stanovit si stupnici a hodnotící kritéria. Stupnice může být vyjádřena penězi, kvalitativními hodnotami nebo kombinací obou (2).

Následující text vychází ze zdroje (2).

[7] Např. metodika CRAMM (CCTA Risk Analysis and Management Method) nebo nová metodika RAC RAMSES a nástroj metodiku využívající RAMSES (Risk Analysis and Management System for Enhanced Security). RAMSES vychází z doporučení normy ISO/IEC 27005, Zdroj: http://www.rac.cz/rac/homepage.nsf/CZ/Ramses

Příklad typické tabulky s termíny pro kvalitativní hodnocení (při napadení aktiva) jsou:

| | | |
|---|---|---|
| **1** | Žádný dopad | Bezvýznamné riziko |
| **2** | Zanedbatelný dopad | Akceptovatelné riziko |
| **3** | Potíže či finanční ztráty | Nízké riziko |
| **4** | Vážné potíže či podstatné finanční ztráty | Nežádoucí riziko |
| **5** | Existenční potíže | Nepřijatelné riziko |

Tabulka 1: Příklad hodnocení aktiv, zdroj: vlastní tvorba

Jak prezentuje tabulka 1, je vhodné používat i barevné odlišení zejména kvůli rozsáhlejším tabulkám, ve kterých lze snadno ztratit přehled. Hodnocení je dobré provést nejen s majitelem aktiv, ale i s uživatelem aktiva. Zamezí se tak případnému zkreslení jeho hodnoty ze strany majitele aktiva.

Výpočet hodnoty aktiva se provádí mnoha způsoby. Nejjednodušší a nejpoužívanější je však tzv. součtový algoritmus, který má tuto podobu:

$$\frac{(dostupnost + důvěrnost + integrita)}{3}$$

**Hrozby**

Hrozby mohou být způsobeny buď lidským faktorem, nebo mohou přicházet z přírody. Dále lze hrozby rozlišit dle toho, zda přišly náhodně, případně byly způsobeny úmyslně. Z hlediska bezpečnosti je pak důležité zajímat se o hrozby náhodné a to tak, že je identifikujeme, odhadneme jejich úroveň a pravděpodobnost.

V praxi je doporučeno seskupit si hrozby podle toho, na jaké aktivum působí:

- operační systém,
- aplikace,
- databáze,
- síť,
- klient.

Posuzování hrozeb provádíme vždy v závislosti na následujících otázkách:

- Ztráta důvěrnosti – může vést ke ztrátě důvěry vůči zákazníkům.
- Ztráta integrity – může vést k přijetí nesprávných rozhodnutí.
- Ztráta dostupnosti – neschopnost vykonávat kritické činnosti.
- Ztráta individuální odpovědnosti – může vést k podvodu.
- Ztráta autentičnosti – může vést k použití neplatných dat.
- Ztráta spolehlivosti – může vést k nespolehlivým dodavatelům.

Důležité je nezapomínat i na tzv. následné efekty hrozby. Příkladem může být výpadek elektrické energie. Kdy výpadek neznamená jen nedostupnost dat, ale při dlouhodobému výpadku může vést až k ohrožení činnosti organizace (v nemocnicích, hasiči, …).

Ochranná opatření postihují tři aspekty: dopady, hrozby a zranitelnosti. Hlavním cílem ochranných opatření je snížit riziko hrozby.

Pro získání představy o hrozbách jsou v normách uváděny seznamy nejčastějších hrozeb.

**Metodiky analýzy rizik**

Rizika rozlišujeme:

- Bezvýznamná – je možné jej přijmout, ale zároveň se nejedná o úplnou bezpečnost, a proto se musí na riziko upozornit a uvést k němu organizační nebo výchovná opatření.
- Akceptovatelná – riziko je přijatelné se souhlasem vedení, zvažují se technická nebo organizační opatření.
- Mírná – zde už je třeba zavést nápravnou činnost, ale zároveň riziko není nijak zvlášť urgentní.
- Nežádoucí – ke snížení tohoto rizika je nutno zavést opatření.
- Nepřijatelná – toto riziko je kritické a práce nesmí být zahájena nebo v ní nesmí být pokračováno, dokud se nesníží.

Metodiky analýzy rizik:

- Hrubá úroveň – na základě analogie podobných systémů a ze všeobecných standardů vytvoříme opatření.
- Neformální přístup - analýzu provedeme na základě znalostí odborníků na bezpečnost bez použití standardních metod.
- Kombinovaný přístup - v jednotlivých oblastech analýzy použijeme podle nutnosti či uvážení elementární, neformální nebo detailní analýzu rizik.
- Podrobný přístup - analýzu provedeme za použití standardních strukturovaných metod ve všech fázích analýzy.

Na použité metodice příliš nezáleží, ale je vhodné postupovat takto:

1. Počáteční analýza rizik pro všechny systémy IT – hrubá úroveň,
2. Systémy významné pro činnost organizace – podrobný přístup.

### Řízení rizik

Cílem řízení rizik je identifikace a kvantifikace rizik, kterým je třeba čelit a poté vhodným způsobem rozhodnout o jejich zvládnutí. Nejčastější metoda je metoda snižování rizik.

Řízení rizik je proces, který se skládá z několika na sebe navazujících fází. Na obrázku 4 je zachyceno, jak tento koloběh etap probíhá.


Obrázek 4: Fáze řízení rizik, zdroj: vlastní tvorba dle (2)

Fáze stanovení kontextu vymezuje oblasti řízení rizik, popisuje tento proces, definuje role a odpovědnosti v procesu, vybírá metodiku pro analýzu rizik, stanovuje referenční úrovně, kritéria a stanovuje míry rizik. V druhém stupni se identifikují a kvantifikují aktiva, hrozby a zranitelnosti a stanovuje se míra rizika. Vyhodnocení rizika je fáze prioritizace rizik a výběru optimálních opatření ke snížení rizika. Závěrečná fáze rozhoduje o vhodném způsobu zvládání rizik (retence, redukce, transfer, pojištění atd.).

Pro správné pochopení problematiky slouží norma ISO/IEC 27005, která se řízení rizik věnuje. Plán zvládání rizik lze nalézt v normě ISO/IEC 27001.

**Opatření**

Jestliže máme hotové všechny přechozí kroky, nezbývá nic jiného, než nastavit opatření na identifikovaná a ohodnocená rizika. K dosažení odpovídající ochrany je možno využít katalogy ochranných opatření, které ukazují na nejčastější obecná opatření k ochraně systému IT.

Opatření rozlišujeme:

- preventivní,
- detekce a reakce,
- podpůrná.

Princip ochranných bezpečnostních opatření spočívá v minimalizaci případných rizik.

V normě ISO/IEC 27005 se nachází tzv. všeobecně aplikovatelná ochranná opatření:

- řízení politiky bezpečnosti IT,
- kontrola bezpečnostní shody,
- řešení incidentů,
- personální opatření,
- provozní problémy,
- plánování kontinuity činnosti organizace,
- fyzická bezpečnost.

V normě ISO/IEC 27002 lze nalézt další ucelený seznam. Norma uvádí celkem 14 oblastí, kdy v každé oblasti je uvedeno opatření a další informace. Ucelený přehled oblastí obsahuje nákres, viz Obrázek 3.

## 3.4 Informační bezpečnost ve zdravotnictví

Jelikož zdravotnické informace jsou považovány za nejdůvěrnější ze všech druhů osobních informací, je nutné věnovat zabezpečení těchto dat mimořádnou pozornost. Ve zdravotnickém sektoru navíc musí být splněny zvláštní požadavky, aby byla zajištěna důvěrnost, integrita, dostupnost a auditovatelnost osobních zdravotnických informací. Specifické nároky bývají kladeny také na informační systémy. Musí být akceschopné při různých systémových selháních či při útocích typu odmítnutí služby. V dnešní době navíc stoupá počet zařízení, která se připojují bezdrátově. Objevují se stále nové technologie, přibývá také personálu pracujícího na dálku nebo si zaměstnanci nosí svá vlastní vybavení[8]. Všechny tyto důvody stále více podněcují organizace, aby do své strategie zavedly také management bezpečnosti.

Pokud se zdravotnická organizace rozhodne ISMS zavést, může k doplnění využít právě zdravotnickou normu ISO/IEC 27779. Tato norma slouží jako doplněk k normě ISO/IEC 27002, rozhodně není určena jako její náhrada (9).

Přímo v normě ISO 27799 je uvedeno, že:

„*Organizace, které zpracovávají zdravotnické informace, včetně osobních údajů, musí mít politiku bezpečnosti informací, která je schválena vedením, publikována a sdělena všem zaměstnancům a příslušným vnějším stranám.“* (9)

ISMS ve zdravotnictví zavádí další pojmy, které je třeba definovat. Následující definice jsou převzaty ze zdroje (2).

**Zdravotnická informatika** (Health informatics) - vědecká disciplína, která se zabývá poznávacími, informačně-zpracovatelskými a komunikačními úkoly zdravotnické praxe, vzděláním a výzkumem včetně informační vědy a technologií na podporu těchto úkolů.

[8] Tzv. BYOD (z angl. Bring Your Own Device)

**Zdravotnický informační systém** (Health informatics system) - je úložiště (repositář) informací týkajících se zdravotního stavu subjektu. Péče v počítačově zpracovatelné formě, uložených a přenášených bezpečně, a přístupných více autorizovaným uživatelům.

**Osobní zdravotní informace** (Personal health information) – jsou informace o identifikovatelné osobě, které se vztahují na fyzické nebo duševní zdraví jedince nebo na poskytování zdravotních služeb jednotlivé osobě. Mohou zahrnovat:

- Informace o registraci jednotlivce pro poskytování zdravotních služeb.
- Informace o platbách nebo nároku na zdravotní péči.
- Číslo, symbol nebo zvláštní označení k jednoznačné identifikaci jednotlivce pro zdravotní účely.
- Veškeré informace o jednotlivci, které byly shromážděny v průběhu poskytování zdravotních služeb.
- Informace získané testováním nebo vyšetřením části těla či tělesné látky.
- Identifikační údaje o osobě jako poskytovateli zdravotní péče.

Zdravotnické informace, které je třeba chránit:

- osobní zdravotní informace,
- pseudonymizovaná data,
- statistické a výzkumné údaje,
- klinické lékařské znalosti,
- údaje o zaměstnancích,
- data auditních záznamů,
- systémová bezpečnostní data.

Z pohledu bezpečnosti zdravotních informací jsou definována tato aktiva:

- lékařské informace,
- služby IT,
- HW,

- SW,
- komunikační zařízení,
- média (nosiče dat),
- IT zařízení,
- lékařská zařízení, která zaznamenávají nebo poskytují data.

Více o normách a zákonech, které souvisí se zdravotnictvím obsahují kapitoly 3.5 a 3.6.

## 3.5 Normy

Tato kapitola pojednává o normách související s danou problematikou. Normy jsou vydány společností ISO. Ta má sídlo ve švýcarském městě Ženeva. Společnost vydala více než 21 tisíc standardů a souvisejících dokumentů, které pokrývají oblasti průmyslu, technologií, potravinářství, zdravotnictví a další (10).

Správa norem v České republice spadá do kompetence Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví. Více se o této instituci zmiňuji v kapitole 3.6.3.

### 3.5.1 Normy řady 27000

ISO rezervovala sérii 27000 pro normy z oblasti bezpečnosti informací. Všechny standardy mají definovanou jednotnou strukturu a pravidla pro začlenění specifických požadavků. Použití této rodiny standardů pomáhá organizacím spravovat bezpečnost majetku, jako jsou finanční informace, duševní vlastnictví, detaily zaměstnanců nebo informace, které organizacím byly svěřeny třetími stranami. Nejznámější standard je ISO/IEC 27001, která poskytuje požadavky na systém řízení bezpečnosti informací (ISMS). V rodině 27K je v současnosti platných 25 standardů a další se připravují (10).

Celý název této normy je *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. V době tvorby této práce je v Česku platná verze z října 2014 a má celkem 31 stran. Nejnovější anglická verze je z roku 2016. S datem 1. června 2017 nabude v účinnost nová verze v angličtině (11).

### 3.5.2 ISO/IEC 27001

Norma s názvem *Systém řízení bezpečnosti informací – Požadavky* vychází z britského standardu BS 7799-2. Poslední revize normy byla publikována v říjnu 2013 (do češtiny přeložena v září 2014). Norma je určena pro malé, střední i velké podniky a pomáhá naplnit bezpečnostní cíle organizace. Poskytuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací (11).

V normě jsou specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva. Chce-li organizace dosáhnout shody s touto normou, je důležité žádné ze specifikovaných požadavků nevynechat. V příloze se nachází přehledná tabulka Cíle opatření a jednotlivá opatření. Opatření jsou přímo odvozena a propojena s těmi, která se uvádí v kapitolách 5 až 18 normy ISO/IEC 27002:2014. Musí být použita v kontextu kapitoly 6.1.3 (6).

Česká verze normy obsahuje 25 stran.

### 3.5.3 ISO/IEC 27002

Tato norma poskytuje pokyny pro zabezpečení bezpečnosti informací a postupy řízení bezpečnosti informací, včetně výběru, implementace a řízení kontrol s přihlédnutím k jejich konkrétnímu prostředí rizik pro bezpečnost informací.

Je určena pro organizace, které hodlají (10):

- Vybrat kontroly v rámci implementace systému řízení bezpečnosti informací založeného na ISO/IEC 27001.
- Provádět obecně uznávané kontroly bezpečnosti informací.
- Vypracovat vlastní pokyny pro řízení informační bezpečnosti.

Bezpečnosti informací je možné dosáhnout zavedením vhodné sady opatření, včetně politik, procesů, postupů, organizačních struktur a softwarových a hardwarových funkcí. Tato opatření je třeba stanovit, implementovat, monitorovat a přezkoumávat. A především zlepšovat tam, kde je nutné, aby bylo zajištěno, že jsou splněny specifické cíle bezpečnosti a podnikatelské činnosti organizace (11).

Celý název normy je *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* V české podobě má norma 73 stran. Doposud je platná verze, která byla vydána v roce 2013 (do češtiny přeložena v roce 2014). Norma obsahuje 14 kapitol týkajících se opatření bezpečnosti společně obsahujících celkem 35 hlavních kategorií bezpečnosti a 114 kontrol (12).

### 3.5.4 ISO/IEC 27799

Norma je doprovodem normy ISO/IEC 27799. Poskytuje pokyny pro standardy bezpečnosti informací a postupy řízení informační bezpečnosti včetně výběru, implementace a řízení kontrol s přihlédnutím k prostředí rizik. Norma nese název *Zdravotnická informatika - Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.*

Definuje pokyny pro podporu interpretace a implementace ve zdravotnické informatice ISO/IEC 27002. Je doprovázejícím mezinárodním standardem.

Norma poskytuje pokyny pro provádění kontrol popsaných v normě ISO/IEC 27002 a v případě potřeby je doplňuje, aby bylo možné je efektivně využívat ke správě zdravotní informační bezpečnosti. Zavedením normy ISO/IEC 27799 budou zdravotnické organizace a další správci zdravotnických informací schopny zajistit minimální požadovanou úroveň bezpečnosti. A to takovou, která je přiměřená okolnostem organizace a která zachová důvěrnost, integritu a dostupnost osobních zdravotních informací v jejich péči.

Vztahuje se na zdravotní informace ve všech jeho aspektech bez ohledu na to, jakým způsobem jsou informace získávány (slovní a číselné, zvukové záznamy, kresby, video a lékařské snímky). Dále jaké prostředky se používají k jejich ukládání (tisk nebo zápis na papír nebo elektronické uložení) a na způsob jeho přenosu (ručně, faxem, přes počítačovou síť nebo poštou), protože informace musí být vždy vhodně chráněny.

ISO/IEC 27799 a ISO/IEC 27002 společně definují, co je požadováno z hlediska bezpečnosti informací ve zdravotnictví, ale neurčují, jak mají být tyto požadavky splněny. Norma se snaží být co nejvíce technologicky neutrální. Neutralita s ohledem na implementační technologie je důležitou vlastností, protože bezpečnostní technologie stále

procházejí rychlým vývojem. Naproti tomu se u mezinárodních standardů, přestože podléhají pravidelnému přezkumu, očekává, že zůstanou po celé roky platné. Stejně tak je důležité, že technologická neutralita ponechává dodavatelům a poskytovatelům služeb možnost navrhnout nové nebo vyvíjející se technologie splňující nepostradatelné, normou popisované, požadavky. Jak je uvedeno v úvodu, obeznámenost s ISO/IEC 27002 je nezbytná pro pochopení této dodatkové normy.

Do oblasti působnosti normy ISO/IEC 27799 nespadají následující oblasti:

A) metodiky a statistické testy pro účinnou anonymizaci osobních zdravotních informací,

B) metodiky pseudonymizace osobních zdravotních informací,

C) kvalita služeb a metody měření dostupnosti sítí používaných pro zdravotní informatiku,

D) kvalita dat (na rozdíl od integrity dat).

Text je převzatý z (10).

V době psaní práce pozbyla platnosti norma z roku 2010, která byla přeložena do češtiny. Od data 1. března 2017 nabyla účinnost norma nová. Do češtiny ale není dosud přeložena.

### 3.5.5 Další normy

Následující výčet norem je čerpán z (11).

**ISO/IEC 26003** *Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací* poskytuje doporučení pro ustanovení a implementaci systému řízení bezpečnosti informací (ISMS) v souladu s požadavky normy ISO/IEC 27001. Norma popisuje proces návrhu a implementace ISMS. Výsledkem je finální plán implementace projektu, na jehož základě lze provést realizaci. Norma nabyla účinnost v roce 2012 a je přeložena z anglického originálu do češtiny.

**ISO/IEC 27004** *Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací – Měření* poskytuje doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření

nebo skupin opatření, jak je uvedeno v ISO/IEC 27001. Implementace těchto doporučení je předmětem programu měření bezpečnosti informací. Norma je z roku 2011 a je přeložena do češtiny.

**ISO/IEC 27005** *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací* poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Nicméně tato mezinárodní norma nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací.

**ISO/IEC 27006** *Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací* specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací.

**ISO/IEC 27007** *Informační technologie - Bezpečnostní techniky - Směrnice pro audit systémů řízení bezpečnosti informací* poskytuje doporučení pro řízení auditů systému řízení bezpečnosti informací a provádění interních nebo externích auditů v souladu s ISO/IEC 27001.

**ISO/IEC 27032** *Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost* poskytuje doporučení pro zlepšení stavu kyberbezpečnosti. Pokrývá základní bezpečnostní postupy pro oblasti, jako jsou bezpečnost informací, sítí, internetu a ochrana kritické informační infrastruktury. Norma poskytuje zejména technická doporučení pro řešení obecných rizik kyberbezpečnosti.

## 3.6 Legislativa a instituce

Při zpracování návrhu bezpečnostní politiky je nutno mít na zřeteli nejen požadavky vyplývající z analýzy rizik, ale také požadavky a povinnosti plynoucí z legislativních úprav ve státě. V této kapitole uvádím stručný přehled základních zákonů, vyhlášek či vládních nařízení. Část je věnována institucícm, které působí v České republice a věnují se problematice bezpečnosti.

### 3.6.1 Zákony

**Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)** je účinný od 1. 1. 2015. Základním cílem zákona je zvýšit bezpečnost kybernetického prostoru a zejména se snažit ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Konkrétní části, které je nutné chránit, jsou prvky kritické informační infrastruktury a významné informační systémy. O významu pojmů je možné dočíst se v nařízení vlády č. 315 o určení prvku kritické infrastruktury a ve vyhlášce č. 316 o kybernetické bezpečnosti (kapitola 3.6.2).

Cílem zákona není řešit všechna rizika v kyberprostoru, jako jsou např. porušování autorských práv, různé podvodné aktivity, úniky elektronických dat či šíření závadného elektronického obsahu. V souvislosti se zákonem vznikla řada nových povinností v oblasti zajištění bezpečnosti. Zákon stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna, určuje způsob reakce na kybernetické hrozby a případně také nasměruje na řešení incidentu.

Kontroly, ukládání nápravných opatření k odstranění nedostatků a případně i udělení sankce za nedodržování povinností je v kompetenci Národního bezpečnostního úřadu (NBÚ).

Zákon v §3 určuje orgány a osoby, kterým ukládá povinnosti v oblasti kybernetické bezpečnosti. Jsou to:

a) Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací (dle 127/2005), pokud nespadá pod písmeno b).
b) Subjekt zajišťující významnou síť, pokud nespadá pod písmeno d).
c) Správce informačního systému kritické informační infrastruktury.
d) Správce komunikačního systému kritické informační infrastruktury.
e) Správce významného informačního systému.

Dne 12. dubna 2017 schválila Poslanecká sněmovna novelu tohoto zákona. Novela rozšiřuje působnost stávajícího zákona na další skupiny provozovatelů nebo správců IT technologií (13).

Znění zákona, dotazy i diskuzní fórum k této problematice lze nalézt na webových stránkách http://www.kybernetickyzakon.cz případně na stránkách NBÚ.

**Zákon č. 101/2001 Sb. o ochraně osobních údajů a o změně některých zákonů** rozlišuje osoby, které zpracovávají osobní údaje jiných lidí (tzv. správce nebo zpracovatel osobních údajů). Dále osoby, jejichž osobní údaje správce a zpracovatele zpracovávají (tzv. subjekty údajů). Správcům a zpracovatelům jsou při ochraně osobních údajů ukládány především povinnosti, zatímco subjektům údajů jsou dána práva. Pro kontrolu dodržování zákona byl zřízen Úřad na ochranu osobních údajů (ÚOOÚ)[9].

**Zákon č. 499/2004 Sb. o archivnictví a spisové službě a změně některých zákonů** (zkráceně Archivní zákon) upravuje státní politiku a formu archivnictví a spisové služby. Je platný od 1. ledna 2005. Zákon určuje, jak evidovat a chránit archiválie, definuje práva a povinnosti vlastníků, držitelů a správců archiválií. Uvedena je i působnost Ministerstva vnitra a dalších správních úřadů[10].

**Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování** vymezuje povinnosti státu, zdravotnických zařízení i uživatelů zdravotnických služeb a zásady zdravotnické péče. Upravuje práva a povinnosti pacientů, osob pacientům blízkých a zdravotních pracovníků[11].

### 3.6.2 Vyhlášky a nařízení

**Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury** definuje odvětví a kritéria, podle nichž lze určit, zda prvek spadá do kritické infrastruktury. Celkem je v tomto nařízení uvedeno 9 oblastí a jeho účinnost je od 1. ledna 2015. Zdroj (14).

[9] Zdroj: www.oou.cz
[10] Zdroj: www.portal.gov.cz
[11] tamtéž

**Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti** (zkráceně vyhláška o kybernetické bezpečnosti) stanovuje strukturu a obsah bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém. Dále určuje bezpečnostní opatření a rozsah jejich zavedení. Představuje kybernetické bezpečnostní incidenty, jejich typy a kategorie. Také udává, jakým způsobem se tyto incidenty nahlašují (15).

**Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES** nabude v platnost 25. května 2018. Toto nařízení (GDPR) je důležitý a přelomový evropský předpis. Dozorový orgán v České republice je Úřad pro ochranu osobních údajů, ale kontroly budou moci provádět i další orgány EU. Nařízení se týká každého subjektu, který zpracovává osobní údaje, ať už svých zaměstnanců, klientů, nebo obchodních partnerů. GDPR je svým dopadem a rozsahem strategickým manažerským projektem, nikoliv pouze technologickým či právním projektem. Za osobní údaje jsou považovány nejen citlivá zdravotnická data či finanční situace jednotlivce, ale také IP adresy nebo cookie soubory. Veškeré zpracování osobních údajů musí být odsouhlaseno. K tomuto odsouhlasení však již nebudou stačit všeobecné podmínky, které jsou často nesrozumitelné a zavádějící.

Dodržováním pravidel uvedených v GDPR by se měla nejen důkladně ochránit data všech osob, ale implicitně ochránit organizaci před vnitřními i vnějšími útoky. GDPR jednoznačně posiluje právo občanů na kontrolu jejich osobních údajů, které je popisují a identifikují (16).

### 3.6.3 Instituce

**Národní bezpečnostní úřad**

Národní bezpečnostní úřad (NBÚ) je orgánem moci výkonné, byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, a to k 1. srpnu 1998.

V říjnu 2011 ustavila vláda České republiky NBÚ gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. NBÚ tuto činnost zabezpečuje prostřednictvím Národního centra kybernetické bezpečnosti (NCKB), jehož součástí je Vládní CERT (GovCERT.CZ).

NBÚ je ústředním správním úřadem pro oblasti:

- ochrany utajovaných informací,
- bezpečnostní způsobilosti,
- kybernetické bezpečnosti.

NBÚ rozhoduje o vydání dokladů o bezpečnostní způsobilosti. Plní úkoly v oblasti ochrany utajovaných informací, povoluje poskytování utajovaných informací v mezinárodním styku, vede ústřední registr a schvaluje zřízení registrů. Dále provádí výkon státního dozoru a ukládá sankce za nedodržení povinností stanovených zákonem. Dále realizuje různé certifikace či zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků[12].

**Národní centrum kybernetické bezpečnosti (NCKB)**

Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.

Hlavní oblasti činnosti centra:

- provozovat Vládní CERT České republiky (GovCERT.CZ),

[12] Zdroj: www.nbu.cz

- spolupráce s ostatními národními CERT® týmy a CSIRT týmy,
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy,
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR,
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti,
- výzkum a vývoj v oblasti kybernetické bezpečnosti[13].

**Vládní CERT** (GovCERT.CZ)

Vládní CERT a týmy typu CSIRT hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti (181/2014 Sb.) a jeho prováděcích předpisů. Úlohou těchto týmů je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Neméně důležitou roli hrají při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

Národní CERT tým zaštiťuje organizace CZ.NIC[14].

**Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ)**

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) byl zřízen zákonem České národní rady č. 20/1993 Sb. o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví. ÚNMZ je organizační složkou státu v resortu Ministerstva průmyslu a obchodu ČR. Hlavním posláním ÚNMZ je zabezpečovat úkoly vyplývající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii. Od roku 2009 zajišťuje také tvorbu a vydávání českých technických norem[15].

[13] Zdroj: https://www.govcert.cz
[14] tamtéž
[15] Zdroj: http://www.unmz.cz/urad/unmz

**České institut pro akreditaci**

Český institut pro akreditaci, obecně prospěšná společnost, jako Národní akreditační orgán založený vládou České republiky poskytuje své služby v souladu s platnými právními předpisy ve všech oblastech akreditace jak státním, tak privátním subjektům[16].

## 3.7 Budoucnost

V této podkapitole chci představit projekt eHealth, který se připravuje a upozornit na dění v oblasti kybernetických bezpečnostních hrozeb.

### 3.7.1 eHealth

Jedná se o nový globální koncept, který využívá informační a telekomunikační technologie k různým zdravotnickým úkonům. Jde zejména o prevenci, diagnostiku, léčbu i podporu veřejného zdraví a zdravého životního stylu.

Patří sem:

- elektronické zdravotní záznamy,
- komunikační infrastruktura pro výměnu důležitých informací,
- podpora telemedicíny (telemonitoring, telekonzultace).

V konceptu nejde pouze o to, aby se do lékařských ambulancí začlenily počítače, ale o to, aby se staly skutečnou součástí postupů obdobně jako krevní testy součástí diagnostiky pacienta. Tento systém je v dnešní moderní době téměř nezbytný. Lidé často cestují. V případě, že se člověk mimo domov ocitne v ohrožení zdraví, je důležité, aby zdravotníci v zahraničí měli přístup k základním informacím o osobě, kterou ošetřují a poskytli jí adekvátní péči.

Další část tohoto konceptu se týká vzdálenému monitorování pacientů. Může se jednat např. o sledování srdečních arytmií, měření tlaku či hladiny cukru v krvi.

[16] Zdroj: http://www.cia.cz

Snaha o zavedení systému v České republice vznikla již v roce 2004. Později, v roce 2007, vznikl *Meziresortní koordinační výbor pro zavedení elektronického zdravotnictví*, který měl za úkol vypracovat odborná stanoviska k rozvoji eHealth v naší zemi. Česko navíc spolupracuje s EU a WHO[17] na přípravách koncepce elektronického zdravotnictví. Prozatím se podařilo zprovoznit některé součásti eHealth. Jsou to např. **eRecept** a **eNeschopenka**. Funkční je také **Národní zdravotnický informační systém**, který spravuje množství národních registrů sloužících ke statistickým i plánovacím a prognostickým účelům. Projekty **MeDiMed** a **ePACS** se zabývají výměnou obrazové dokumentace mezi poskytovateli zdravotních služeb. Známé jsou však i neúspěšné projekty, např. IZIP[18] (17).

V listopadu 2016 byla schválena Národní strategie elektronického zdravotnictví na období 2016 až 2020. V této strategii jsou definovány 4 cíle:

1. zvýšení zainteresovanosti občana na péči o vlastní zdraví, prevence,
2. zvýšení efektivity zdravotnického systému,
3. zvýšení kvality a dostupnosti zdravotních služeb,
4. vytvoření a rozvoj informační infrastruktury a správa elektronického zdravotnictví.

Stát však nebude vytvářet žádný rozsáhlý centralistický projekt, ale zajistí základní stavební kameny elektronizace, které umožní postupný vznik a realizaci účelných dílčích projektů, sladěných se strategickými záměry. Role státu při definovaní koncepce a priorit elektronického zdravotnictví je nezastupitelná (18).

### 3.7.2 Bezpečnostní hrozby

V nedávné době byl globálně rozšířen kybernetický útok, který později získal název WannaCry. Tento malware se během chvíle rozšířil do více než poloviny států světa

[17] WHO (World Health Organisation)
[18] IZIP (Elektronická zdravotní knížka)

a napadl kolem 75 000 společností. Jedná se o populární typ malware známý jako ransomware, kdy útočníci cílí na nezabezpečené stanice s vidinou zbohatnutí.

Malware po napadení stanice zašifruje symetrickou kryptografickou šifrou AES nejen veškerá lokální data, ale také všechna připojená dostupná úložiště jako jsou flash disky nebo síťové NAS[19] servery. Klíč sloužící k možnému dešifrování dat je odeslán útočníkům a z napadené stanice odstraněn.

Na rozdíl od ostatních obdobných malware tento také zneužíval již opravené zranitelnosti v síťovém protokolu Samba běžících na stanicích s operačním systémem MS Windows. Neaktualizované stanice tak byly napadeny automaticky bez nutnosti kooperace uživatele. Především stanice provozující starý nepodporovaný systém Windows XP tak jsou ve velkém ohrožení.

Pokud neexistují zálohy, není jiná možnost než útočníkům zaplatit výkupné ve formě anonymní měny BitCoin. To se však nedoporučuje, protože nejen, že není žádná jistota, že útočníci stanici dešifrují, ale především se zaplacením výkupného podporuje toto odvětví nebezpečného a nekalého vývoje obdobných typů útoků. Mezi napadené stanice patřily právě i neaktualizované systémy zdravotnických organizací (19).

[19] NAS (z angl. Network Attached Storage)

# 4 Analýza současného stavu

V analytické části nejprve představím společnost a prostředí, kde provozuje svoji činnost. Následně provedu rozbor současného stavu zabezpečení informací.

## 4.1 Popis společnosti

Vybraná zdravotnická společnost, pro kterou je tato diplomová práce zpracovávána, si z důvodu ochrany citlivých informací a údajů nepřeje být explicitně jmenována. V práci bude proto organizace označena zástupným jménem gynekologie nebo (zdravotnická) organizace.

Zdravotnické zařízení, které podrobím analýze bezpečnosti, je gynekologická ordinace sídlící v okresním městě.

## 4.2 Situační analýza

Ordinace je umístěna v budově polikliniky. Tato stavba pochází z 90. let 20. století a celkově má 6 pater včetně suterénu. Všechna patra jsou dostupná po schodišti nebo osobními výtahy. Poliklinika sídlí na okraji města v blízkosti řeky. Poskytuje služby zdravotnické (RTG, praktiční lékaři, zubní lékaři atd.) i nezdravotnické (ostraha, ústředna, úklid atd.). Další služby zajišťují subjekty, kterým jsou pronajímány prostory (ordinace soukromých lékařů, lékárna, novinový stánek atd.). Společnost zabezpečuje dodávky energií, úklid a likvidaci odpadů, ostrahu. Dále běžné opravy, servis a údržbu zdravotnického vybavení, telefonní ústřednu a také archivaci zdravotnické dokumentace. Do archivu se ukládá zdravotnická dokumentace zemřelých pacientů nebo těch, kteří byli z nějakého důvodu vyřazeni z evidence. Místnost je uzamčena a přístup má pouze archivářka a ostraha.

### 4.2.1 Parkoviště, vstupy a kamery

S poliklinikou sousedí několik veřejných placených parkovišť. Oplocená parkovací plocha pro zaměstnance přiléhá k budově. Vstupní závoru lze otevřít pomocí čipové karty, dálkového ovládání nebo prostřednictvím zvonku s kamerou, který je napojený na recepci/ostrahu. V zadním traktu se nachází závorou zajištěné parkoviště pro sanitní vozy.

Závoru lze otevřít dálkovým ovládáním či použitím zvonku s kamerou a mikrofonem, kdy je požadováno nahlášení důvodu vjezdu.

Do objektu vedou čtyři vchody. Jeden z nich je zaměstnanecký, propojený s oploceným parkovištěm. Kamery jsou umístěny ve venkovních prostorech (vchody, brány na parkoviště) i na chodbách. Sledování výstupů zajišťuje ostraha. Záznamy se ukládají na nahrávací zařízení pro kamerový systém. Případné vystavení nahraných záznamů obstarává správce sítě.

### 4.2.2 Popis vnitřních prostor polikliniky

Do suterénu je možné vstoupit ze zaměstnaneckého parkoviště a současně z parkoviště pro sanitky. Nachází se zde šatny pro personál, ordinace lékaře a ostatní nezdravotnické služby (kantýna, kosmetika). Do šaten mají přístup zaměstnanci, uklízečka a ostraha. Každý zaměstnanec má svoji skříňku a k ní klíč. V prvním patře se nachází hlavní vchod a recepce. Prostory recepce jsou společné pro recepční i ostrahu. Místnost disponuje obrazovkou, kde jsou centralizovány výstupy všech kamer. Ostatní prostory náleží zdravotnickým subjektům a lékárně. Další tři patra jsou zařízena ambulancemi lékařů. Nejvyšší patro slouží jako zázemí pro vedení společnosti a správu polikliniky. O svátcích a víkendech je v provozu pouze lékárna. Přístup k ní vede pouze bočním vchodem. Ostraha je zajištěna i v nepracovní dny.

### 4.2.3 Gynekologická ambulance

Ordinace gynekologie, kterou se zabývám v této diplomové práci, je provozována v jedné z pronajatých ambulancí třetího patra. Pronajatý prostor se skládá z čekárny, recepce (administrativa), sesterny a dvou ordinací lékařů. Mezi čekárnou a recepcí jsou dveře, které se po skončení pracovní doby uzamykají. Duplicitní klíč mají pracovníci úklidu a ostrahy, které zaměstnává poliklinika. Žádné další dveře se nezamykají.

Uvnitř administrativní části je umístěna kartotéka pro zdravotní záznamy pacientů, která není uzamykatelná. Administrativa personálních a účetnických dokumentů sídlí mimo objekt polikliniky v sídle společnosti (sídlo společnosti není totožné s místem provozování ambulance).

Předmět a rozsah činnosti gynekologické ambulance:

- preventivní prohlídky,
- diagnostika a léčba gynekologických obtíží,
- těhotenská poradna,
- urogynekologie,
- poradenství (klimakterické, antikoncepční, …),
- očkování.

Organizace vlastní od roku 2007 certifikát ISO 9001 Management kvality. Jedenkrát ročně je prováděn kontrolní audit a jednou za dva roky přezkoumání.

Webové stránky ambulance jsou pouze informativní (ordinační doba, sídlo, rozsah činnosti apod.).

## 4.3 Analýza IT vybavení a zařízení

Zapojení počítačů a různá nastavení připojení má v kompetenci správce sítě, který je zaměstnancem polikliniky. Nákup hardware, některé opravy IT zařízení či poradenství v této oblasti zajišťuje externí firma.

### 4.3.1 Internetové připojení

Připojení do sítě poskytuje přímo poliklinika. Bezdrátové Wi-Fi připojení pro veřejnost zatím zprovozněno není. Ordinace se v současnosti připravuje na spuštění další vlny EET[20]. Pokladna bude se systémem spojena přes Wi-Fi a veškeré připojení i nákup potřebného hardware zajišťuje externí společnost. Počítače jsou propojeny kabelem do společného switche. Switch je připojen k vlastnímu routeru pro oddělení sítě od hlavní sítě polikliniky. V administrativní části ordinace je umístěn vlastní server HP ProLiant, kam se ukládají všechna data. Na serverech běží standardní řešení operačního systému od společnosti Microsoft. Správa serveru je možná pouze pomocí vzdálené plochy. Zálohování probíhá pomocí kopie dat a obrazu pevného disku na další pevný disk, který se nijak nešifruje. Ordinace prozatím nevyužívá žádnou cloudovou službu.

[20] EET (elektronická evidence tržeb)

### 4.3.2 Zdravotnická a IT zařízení

Ordinace lékařů jsou vybavené zdravotnickými přístroji. Přístroje nejsou nijak propojené mezi sebou, ani nemají zapojení do internetové sítě. Pouze ultrazvuk je připojen přes kabel k jednomu z počítačů lékaře. Celkově má ambulance čtyři počítačové stanice. Jeden má k dispozici recepční, další se nachází v sesterně. Každá z ordinací pak disponuje po jednom počítači pro lékaře. Ke všem počítačům (včetně serveru) je navíc připojen zdroj nepřerušovaného napájení tzv. UPS[21], které v případě výpadku proudu zamezí ztrátě důležitých dat.


Obrázek 5: Zdroj nepřerušovaného napájení, zdroj: vlastní fotografie

Počítače jsou chráněny přístupovými hesly k jednotlivým účtům a běží na nich operační systém Windows (v počítačích pro administrativu a pro sestry se nachází Windows XP, u lékařů se jedná o distribuci Windows 7). Nejedná se tedy o centralizované řízení přístupu typu Active Directory. Na počítačích je nainstalováno komerční řešení antivirového softwaru Kaspersky, který se sám aktualizuje. Systémy nepodléhají žádnému omezení z pohledu manipulace s daty či datovými nosiči včetně USB flashdisků. Přístup k Internetu, i možnost stahovat jakákoliv data, lze na všech počítačích. Tiskárny se v ambulanci nachází celkem čtyři, z nichž po jednom kusu je v ordinacích

[21] UPS (z anglického Uninterruptible Power Supply/Source)

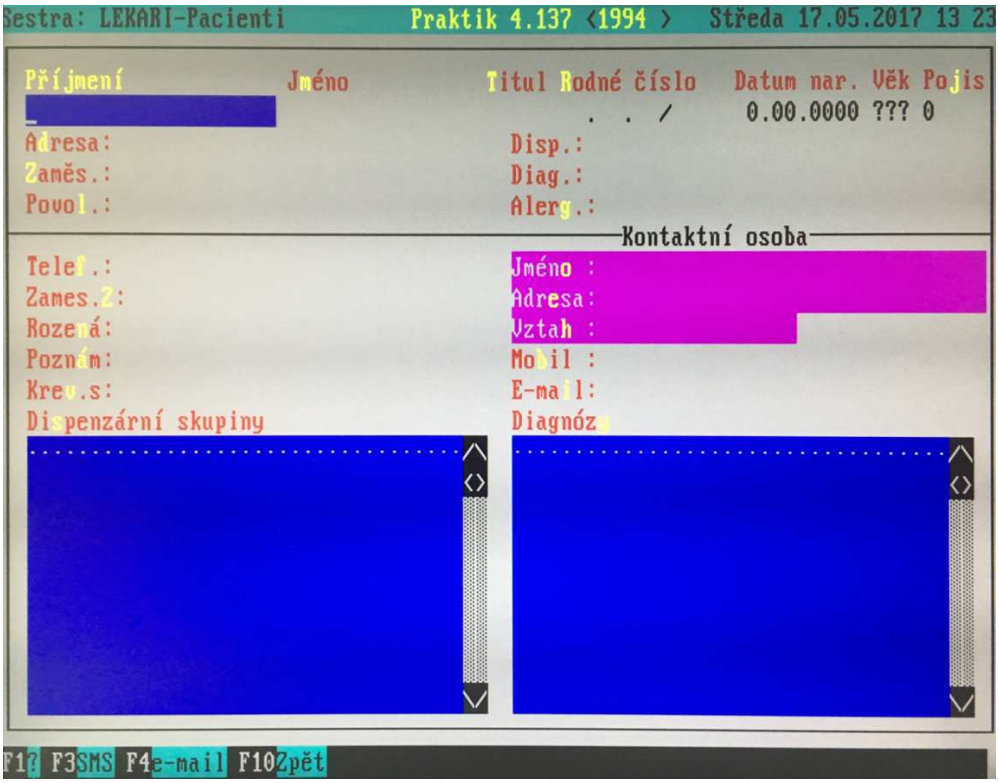
lékařů a dvě jsou připojené k počítači na recepci (jedna pro tisk receptů a dokumentů z informačního systému, druhá pouze pro kopírování). Tiskárny nejsou síťové.

Do počítače pro lékaře je možné připojit čidlo, které kontroluje teplotu v lednici. V lednici se uchovávají některá léčiva a očkovací látky. Přístup nepovolaným osobám je zamezen zámkem.

Do ambulance je zavedena pevná telefonní linka. Využívá se nejen pro komunikaci s pacienty, ale také pro přepojení na jiná oddělení přes ústřednu polikliniky. V prostoru recepce je umístěn také skartovací přístroj.

### 4.3.3 Softwarové vybavení

V ordinaci je využíván informační systém PRAKTIK. V tomto systému je vedena zdravotnická dokumentace. Dokumentace se také vždy tiskne a poté v papírové podobě zakládá do kartotéky. Systém umožňuje rovněž tisk receptů, žádanek či dalších formulářů. Obsahuje modul „zvací systém“, který upozorňuje sestry k pozvání pacientek na kontrolní nebo preventivní vyšetření. Dále se zde nachází databáze léčiv a různé statistické nástroje, které využívají zejména lékaři. Přímo ze systému je pak možné tisknout sestavy pro zdravotní pojišťovny. Informační systém obsahuje rozhraní, pomocí kterého odesílá laboratoř výsledky laboratorních testů online.



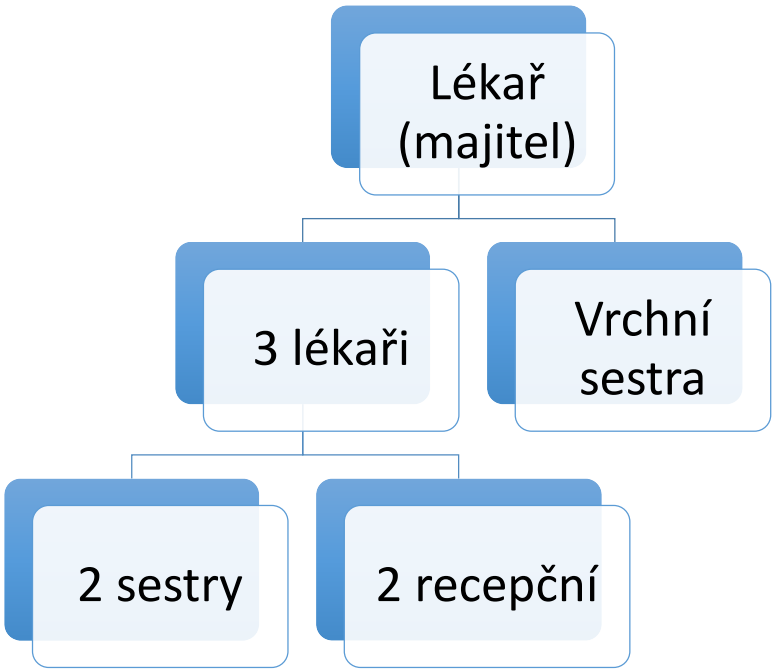

Obrázek 6: Informační systém PRAKTIK, zdroj: vlastní fotografie

Administrativě jsou přístupné také dvě databáze, ke kterým se přihlašuje pomocí webového rozhraní. Jedna databáze obsahuje laboratorní výsledky, druhá databáze umožňuje objednávat pacientky na mamografické vyšetření.

E-mailovou komunikaci využívá zejména hlavní lékař (majitel ordinace). Na jeho počítači je instalován Microsoft Outlook 2010. Sestry i administrativa používají v případě potřeby svoje osobní e-maily, protože řešení od Microsoftu není plně v provozu. Převážná část komunikace je ale osobní, telefonická nebo se zasílají výsledky a žádanky prostřednictvím České pošty.

## 4.4 Personální situace

Do ambulance byl zakoupen přístroj pro zaznamenávání příchodů a odchodů personálu ze zaměstnání. Tento docházkový systém funguje na principu otisku prstů a prozatím se nachází v testovacím režimu. Plánuje se jeho připojení k počítači, kde bude veden o docházce přehled.




Obrázek 7: Schéma personálního složení organizace, zdroj: vlastní zpracování

Hlavní lékař (zároveň majitel společnosti) má ordinační dobu v pondělí a ve středu.

Jeden lékař ordinuje každý den a další se střídají. Stabilně je v ordinaci jedna sestra a jedna recepční (administrativa). Ostatní sestry a administrativa zde pracují pouze jako zástup v případě nemoci nebo dovolené zaměstnanců na hlavní pracovní poměr. Některé sestry a administrativa zde tedy působí na základě DPP či DPČ.[22]

Vrchní sestra pracuje zejména pro polikliniku. Do ordinace však chodí jako zástup a současně v ní působí také jako manažer kvality. Její kancelář se nachází v posledním patře polikliniky, kam se lze dostat pouze po zazvonění a odůvodnění vstupu.

Při náboru nových zaměstnanců jsou kladeny náročnější požadavky. Administrativa musí mít povědomost o lékařských postupech, rozumět diagnóze, výsledkům různých testů. Kladen je důraz na dobré jednání s lidmi. U sester se předpokládá odpovídající vzdělání. Výhodou je praxe v oboru porodní asistentka.

Při nástupu do zaměstnání podepisují pracovníci smlouvu, ve které je zakotvena smlouva o mlčenlivosti. Po zahájení pracovního procesu jsou zaměstnanci důkladně proškoleni

[22] DPP (Dohoda o provedení práce), DPČ (Dohoda o pracovní činnosti)

a seznámeni s chodem ordinace. Všichni mají také k dispozici dokumentaci ISO 9001, která je uložena u vrchní sestry (manažer kvality) v papírové i elektronické formě. V ambulanci se nachází kopie dokumentace. Pracovníkům je nutné zabezpečit školení BOZP a zároveň také vstupní proškolení k obsluze přístrojů (zejména zdravotní personál).

# 5 Vlastní návrh řešení

Na základě analýzy organizace, provedené osobně přímo na pracovišti, jsem zjistila, že největší nedostatky jsou v IT a oblasti fyzické. Chybí také proškolení zaměstnanců v souvislosti bezpečnosti informací. Budovat bezpečnostní povědomí u zaměstnanců považuji za velmi důležité.

V praktické části diplomové práce nejdříve identifikuji a ohodnotím aktiva. Následovat bude analýza rizik, hodnocení jejich dopadu a návrh na opatření pro snížení dopadů těchto rizik. Cílem je poukázat na možná rizika a navrhnout opatření. Dále stanovení rámce pro řízení, prosazování a kontrolu bezpečnosti informací v rámci zkoumané organizace. Mým záměrem však není detailní analýza bezpečnostní politiky organizace, ale zmapování současného stavu v oblasti zabezpečení informací.

## 5.1 Identifikace a hodnocení aktiv

Nejprve jsem nastínila, jaké kategorie aktiv se v organizaci nachází.

Kategorie:

- data,
- interní dokumenty,
- software,
- fyzická aktiva.

Toto členění je dále rozvinuto skupinami aktiv. Ke každé skupině uvádím i umístění, jelikož ne všechna aktiva se nachází přímo v ordinaci.

Navazuje tabulka s přehledem o aktivech a jejich zařazením.

| Pořadí | Kategorie | Skupina | Umístění |
|---|---|---|---|
| 1 | Data | Elektronická zdravotnická dokumentace | Ordinace |
| | | Papírová zdravotnická dokumentace | Ordinace |
| | | Archivovaná (papírová) zdravotnická dokumentace | Poliklinika (archiv) |
| | | Personální a účetnická data | Účetní |
| | | Zálohy na serveru | Ordinace |
| 2 | Interní dokumenty | Směrnice pro provoz zdravotnického zařízení | Ordinace |
| | | Dokumentace ISO 9001 - papírová | Vrchní sestra |
| | | Dokumentace ISO 9001 - elektronická | Vrchní sestra |
| | | Dodavatelské smlouvy | Vrchní sestra |
| 3 | Software | Informační systém PRAKTIK | Ordinace |
| | | Operační systém | Ordinace |
| 4 | Fyzická aktiva | Počítače | Ordinace |
| | | Periferní zařízení (UPS, tiskárny) | Ordinace |
| | | Zdravotnická (vyšetřovací) zařízení | Ordinace |
| | | Server | Ordinace |
| | | Lednice pro léčiva | Ordinace |
| | | Aktivní síťové prvky | Ordinace |

Tabulka 2: Seznam aktiv, zdroj: vlastní zpracování

V dalším kroku následuje hodnocení stanovených aktiv. Aktiva jsou ohodnocena na základě posouzení požadavků na dostupnost, integritu a důvěrnost dat.

Po diskuzi s lékařem (majitelem) a uživateli aktiv (sestry, administrativa) vznikla následující Tabulka 3.

Stanovená škála hodnotících kritérií: 1 až 5 (5 jsou nejdůležitější aktiva). Pro větší přehlednost jsou hodnoty aktiv rozlišeny barvami.

| Skupina | Dostupnost | Důvěrnost | Integrita | Hodnota |
|---|---|---|---|---|
| Elektronická zdravotnická dokumentace | 5 | 5 | 5 | 5 |
| Papírová zdravotnická dokumentace | 2 | 5 | 4 | 4 |
| Archivovaná (papírová) zdravotnická dokumentace | 2 | 5 | 4 | 4 |
| Personální a účetní data | 2 | 5 | 3 | 3 |
| Zálohy na serveru | 4 | 5 | 4 | 4 |
| Směrnice pro provoz zdravotnického zařízení | 3 | 3 | 4 | 3 |
| Dokumentace ISO 9001 - papírová | 3 | 5 | 4 | 4 |
| Dokumentace ISO 9001 - elektronická | 3 | 5 | 4 | 4 |
| Dodavatelské smlouvy | 3 | 5 | 5 | 4 |
| Informační systém PRAKTIK | 5 | 5 | 5 | 5 |
| Operační systém | 5 | 5 | 5 | 5 |
| Počítače | 3 | 5 | 4 | 4 |
| Periferní zařízení (UPS, tiskárny) | 2 | 2 | 3 | 2 |
| Zdravotnická (vyšetřovací) zařízení | 3 | 4 | 4 | 4 |
| Server | 5 | 5 | 5 | 5 |
| Lednice pro léčiva | 3 | 5 | 5 | 4 |
| Aktivní síťové prvky | 4 | 5 | 5 | 5 |

Tabulka 3: Hodnocení aktiv, zdroj: vlastní zpracování

Na základě provedeného hodnocení vyplývá, že nejvyšší nároky na důvěrnost, integritu a dostupnost mají tato aktiva:

- elektronická zdravotnická dokumentace,
- informační systém PRAKTIK,

- operační systém,
- server,
- aktivní síťové prvky.

## 5.2 Identifikace hrozeb a zranitelností

Dalším předpokladem pro úspěšnou analýzu rizik je identifikace a ohodnocení hrozeb, které působí nebo mohou působit na prověřovanou společnost. Je důležité stanovit stupnici pravděpodobnosti, se kterou se hrozba může objevit.

Tabulka 4 obsahuje měřítko pravděpodobnosti vzniku hrozby, které bude použito k ohodnocení hrozeb společnosti.

| **Pravděpodobnost hrozby** | **Označení** | **Popis** |
|---|---|---|
| Velmi nízká | 1 | Velmi nízká pravděpodobnost, zanedbatelný dopad |
| Nízká | 2 | Nízká pravděpodobnost, zanedbatelný dopad |
| Středně vysoká | 3 | Středně vysoká pravděpodobnost, nezanedbatelný dopad |
| Vysoká | 4 | Vysoká pravděpodobnost, ohrožení chodu společnosti |
| Velmi vysoká | 5 | Velmi vysoká pravděpodobnost, zásadní dopad na chod společnosti |

Tabulka 4: Pravděpodobnost vzniku hrozby, zdroj: vlastní zpracování

Tabulka 5 zobrazuje současně pravděpodobnost vzniku hrozby a příklad zranitelnosti. Stupnice je opět zvolena na škále od 1 do 5, viz. Tabulka 4.

| Druh hrozby | Hrozba | Celkové hodnocení |
|---|---|---|
| Přírodní, fyzické | Poškození ohněm | 1 |
| | Poškození vodou | 3 |
| | Kolísání dodávek elektřiny | 3 |
| | Lidské katastrofy (terorismus) | 2 |
| Technologické, technické | Počítačový virus | 4 |
| | Selhání softwaru | 5 |
| | Selhání připojení | 3 |
| | Selhání hardwaru | 3 |
| | Odposlouchávání komunikací | 4 |
| | Neoprávněný přístup | 5 |
| Lidské | Falšování identity | 3 |
| | Selhání údržby IT | 3 |
| | Chyba uživatele | 4 |
| | Krádež dat | 4 |
| | Úmyslné poškození | 2 |
| | Vyzrazení tajných informací | 3 |

Tabulka 5: Ohodnocení hrozeb s pravděpodobnostmi výskytu, zdroj: vlastní zpracování

Hrozby jsou rozděleny do tří kategorií. Ke každému typu pak uvádím konkrétní příklad. Abych vyloučila možnost přehlédnutí některé z hrozeb, řídila jsem se přílohou A v normě ISO 27799. Norma shrnuje nejčastější a nezávažnější typy hrozeb, které mohou způsobit škody zdravotnické organizaci.

Na základě předchozích dvou analýz jsem sestavila matici zranitelnosti V. Tu reprezentuje Tabulka 6. Matice vyjadřuje velikost pravděpodobnosti ohrožení aktiva konkrétní hrozbou. V matici figurují aktiva organizace a možné hrozby na ně působící. Mezi nimi je pak na stupnici 1 až 5 zobrazena hodnota zranitelnosti. Čím vyšší hodnota, tím větší zranitelnost.

| V | ← A | Poškození ohněm | Poškození vodou | Kolísání dodávek | Lidské katastrofy | Počítačový virus | Selhání softwaru | Selhání připojení | Selhání hardwaru | Odposlouchávání | Neoprávněný přístup | Falšování identity | Selhání údržby IT | Chyba uživatele | Krádež dat | Úmyslné poškození | Vyzrazení tajných |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **T →** | | **1** | **3** | **3** | **2** | **4** | **5** | **3** | **3** | **4** | **5** | **3** | **3** | **4** | **4** | **2** | **3** |
| El. dokumentace | **5** | 1 | 1 | 3 | 2 | 5 | 5 | 4 | 4 | 4 | 5 | 4 | 4 | 5 | 5 | 4 | 5 |
| Papír. dokumentace | **4** | 5 | 5 | | 3 | | | | | | 5 | 5 | 3 | 5 | 5 | 4 | 5 |
| Archiv | **4** | 3 | 3 | | 2 | | | | | | 5 | 5 | 1 | 3 | 5 | 4 | 5 |
| Person. a účet. data | **3** | 4 | 4 | | 3 | 3 | 2 | 1 | 1 | 2 | 4 | 3 | 1 | 5 | 4 | 4 | 5 |
| Zálohy | **4** | 2 | 2 | 5 | 3 | 5 | 4 | 4 | 5 | 4 | 5 | 3 | 5 | 4 | 4 | 4 | 4 |
| Směrnice | **3** | 1 | 1 | | 2 | | | | | | 3 | 3 | | 2 | 2 | 2 | 1 |
| ISO papír. | **4** | 1 | 1 | | 2 | | | | | | 2 | 4 | | 2 | 3 | 2 | 1 |
| ISO el. | **4** | 1 | 1 | | 1 | 3 | 2 | 1 | 2 | 2 | 3 | 3 | 1 | 2 | 3 | 2 | 1 |
| Smlouvy | **4** | 2 | 2 | | 2 | | | | | | 3 | 3 | | 2 | 3 | 2 | 3 |
| IS | **5** | | | 4 | 2 | 4 | 5 | 3 | 4 | 5 | 5 | 4 | 5 | 4 | 5 | 3 | 3 |
| OS | **5** | | | 3 | 2 | 5 | 4 | 4 | 3 | 3 | 4 | 2 | 4 | 4 | 2 | 3 | 1 |
| Počítače | **4** | 2 | 2 | 5 | 2 | 4 | | | 4 | 2 | 4 | 4 | 4 | 4 | | 3 | 1 |
| Periferie | **2** | 1 | 1 | 3 | 2 | 2 | | | 3 | | | 1 | 2 | 2 | | 1 | |
| Zdrav. zařízení | **4** | 2 | 2 | 3 | 3 | | | | | | | 4 | | 4 | | | |
| Server | **5** | 3 | 3 | 5 | 3 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 2 | 5 | 4 | 3 |
| Lednice | **4** | 1 | 1 | 4 | 1 | | | | | | 5 | 4 | | 1 | | | |
| Síť. prvky | **5** | 2 | 2 | 4 | 2 | 3 | 3 | 4 | 3 | 3 | 4 | 4 | 4 | 2 | | 2 | 2 |

Tabulka 6: Matice zranitelnosti, zdroj: vlastní zpracování

## 5.3 Míry rizik

Následuje krok, kdy je potřeba vytvořit matici rizik R. Způsob, jak vypočítat míru rizika je následující:

$$R = T \cdot A \cdot V ,$$

kde:

- R – míra rizik,
- T – pravděpodobnost vzniku hrozby,
- A – hodnota aktiva,
- V – zranitelnost aktiva.

Kategorie míry rizik jsem stanovila takto:

| **Rozmezí** | **Kategorie** |
|---|---|
| 0 až 35 | Nízké riziko |
| 36 až 74 | Středně vysoké riziko |
| 74 a více | Vysoké riziko |

Tabulka 7: Kategorie míry rizik, zdroj: vlastní zpracování

Při nejvyšší pravděpodobnosti hrozby (5), nejvyšší hodnotě aktiva (5) a největší zranitelnosti (5) je dosaženo maximální výsledné hodnoty, která dosahuje úrovně 125.

Tabulka 8 představuje matici rizik R a vychází z předchozích získaných hodnot.

| R | ← A | Poškození ohněm | Poškození vodou | Kolísání dodávek el. | Lidské katastrofy | Počítačový virus | Selhání softwaru | Selhání připojení | Selhání hardwaru | Odposlouchávání | Neoprávněný přístup | Falšování identity | Selhání údržby IT | Chyba uživatele | Krádež dat | Úmyslné poškození | Vyzrazení tajných |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **T →** | | **1** | **3** | **3** | **2** | **4** | **5** | **3** | **3** | **4** | **5** | **3** | **3** | **4** | **4** | **2** | **3** |
| El. dokumentace | **5** | 5 | 15 | 45 | 20 | 100 | 125 | 60 | 60 | 80 | 125 | 60 | 60 | 100 | 100 | 40 | 75 |
| Papír. dokumentace | **4** | 20 | 60 | | 24 | | | | | | 100 | 60 | 36 | 80 | 80 | 32 | 60 |
| Archiv | **4** | 12 | 36 | | 16 | 48 | 30 | | | | 100 | 60 | 12 | 48 | 80 | 32 | 60 |
| Person. a účet. data | **3** | 12 | 36 | | 18 | 36 | 30 | 9 | 9 | 24 | 60 | 27 | 9 | 60 | 48 | 24 | 45 |
| Zálohy | **4** | 8 | 24 | 60 | 24 | 80 | 80 | 48 | 60 | 64 | 100 | 36 | 60 | 64 | 64 | 32 | 48 |
| Směrnice | **3** | 3 | 9 | | 12 | | | | | | 45 | 27 | | 24 | 24 | 12 | 9 |
| ISO papír. | **4** | 4 | 12 | | 16 | | | | | | 40 | 48 | | 32 | 48 | 16 | 12 |
| ISO el. | **4** | 4 | 12 | | 8 | 48 | 48 | 12 | 24 | 32 | 60 | 36 | 12 | 32 | 48 | 16 | 12 |
| Smlouvy | **4** | 8 | 24 | | 16 | | | | | | 60 | 36 | | 32 | 48 | 16 | 36 |
| IS | **5** | | | 60 | 20 | 80 | 125 | 45 | 60 | 100 | 125 | 60 | 75 | 80 | 100 | 30 | 45 |
| OS | **5** | | | 45 | 20 | 100 | 100 | 60 | 45 | 60 | 100 | 30 | 60 | 80 | 40 | 30 | 15 |
| Počítače | **4** | 8 | 24 | 60 | 16 | 64 | | | 48 | 32 | 80 | 48 | 48 | 64 | | 24 | 12 |
| Periferie | **2** | 2 | 6 | 18 | 8 | 16 | | | 18 | | | 6 | 12 | 16 | | 4 | |
| Zdrav. zařízení | **4** | 8 | 24 | 36 | 24 | | | | | | | 48 | | 64 | | | |
| Server | **5** | 15 | 45 | 75 | 30 | 100 | 100 | 75 | 75 | 100 | 125 | 75 | 75 | 40 | 100 | 40 | 45 |
| Lednice | **4** | 4 | 12 | 48 | 8 | | | | | | 100 | 48 | | 16 | | | |
| Síť. prvky | **5** | 10 | 30 | 60 | 20 | 60 | 75 | 60 | 45 | 60 | 100 | 60 | 60 | 40 | | 20 | 30 |

Tabulka 8: Matice rizik, zdroj: vlastní zpracování

Aby bylo v matici lépe rozpoznat, která rizika mají nejvyšší hodnotu, označila jsem je barvami dle následující tabulky.

| Míra rizika | Typ rizika |
|---|---|
| 0 až 10 | Bezvýznamné riziko |
| 11 až 30 | Akceptovatelné riziko |
| 31 až 50 | Mírné riziko |
| 51 až 70 | Nežádoucí riziko |
| 71 a více | Nepřijatelné riziko |

Tabulka 9: Hodnocení rizik, zdroj: vlastní zpracování

Zmínka o tom, jak uvedené typy rizik řídit, je zmíněna v kapitole 3.3.5 v teoretické části práce.

Z matice vychází, že největší rizika vznikají při působení hrozeb na zdravotnickou dokumentaci v jakékoliv podobě. Zvýšená míra ohrožení se týká informačního a operačního systému, serveru a síťových prvků. Vyjmenovaná aktiva bude tedy nutné zabezpečit s nejvyšší prioritou.

Na základě analýzy v podniku bylo zjištěno, že v některých oblastech zabezpečení jsou stále nedostatky. V následující kapitole proto navrhnu bezpečnostní příručku pro organizaci, která vychází z požadavků normy ISO/IEC 27002.

## 5.4 Bezpečnostní příručka organizace

Účelem příručky je rozpracovat opatření v oblasti řízení bezpečnosti informací a současně se pokusit nastínit důležitost navržených opatření, které by mohly snížit nebo eliminovat nalezená rizika.

Organizace již vlastní certifikaci systému managementu kvality (ISO 9001) a má zavedené postupy v oblasti manažerské a personální. Ve vlastním zájmu by společnost měla usilovat také o certifikaci dle normy ISO/IEC 27001, protože pracuje s důvěrnými daty.

Příručka popisuje opatření vybraná na základě hodnocení rizik v oblastech:

- politiky bezpečnosti informací,
- organizace bezpečnosti informací,
- bezpečnost lidských zdrojů,
- řízení aktiv,
- řízení přístupu,
- fyzická bezpečnost a bezpečnost prostředí,
- bezpečnost provozu,
- bezpečnost komunikací,
- akvizice, vývoj a údržba systému,
- vztahy s dodavateli,
- řízení incidentů,
- aspekty řízení kontinuity činnosti organizace,
- soulad s požadavky.

### 5.4.1 Politiky bezpečnosti informací

Prvním krokem při zavádění ISMS je nutné vedením organizace určit směřování bezpečnosti informací. To v praxi znamená, že management společnosti musí jasně vyjádřit podporu pro zavedení bezpečnosti informací v **dokumentu *Politika bezpečnosti informací*.** Tato podpora musí být v souladu s požadavky týkajícími se činnosti organizace, příslušnými zákony a směrnicemi.

Dokument by měl být schválen vedením organizace, vydán a zpřístupněn všem zaměstnancům a relevantním externím stranám.

V dokumentu by měla být obsažena následující prohlášení:

- definice bezpečnosti informací, cílů a principů, které budou směrovat veškeré činnosti související s bezpečností informací,
- k definovaným rolím přiřazení obecné a specifické odpovědnosti,
- postupy pro zacházení s odchylkami a výjimkami,
- prohlášení o potřebě bezpečnosti zdravotnických informací,

- cíle bezpečnosti zdravotnických informací,
- prohlášení o legislativních, správních a smluvních požadavcích, právní a etické povinnosti odborných zdravotnických pracovníků,
- ujednání o oznamování incidentů bezpečnosti informací.

Obsah politiky bezpečnosti informací musí být sdělen všem zaměstnancům i relevantním externím stranám ve srozumitelné formě. Vhodné je i zařazení prezentace těchto politik do rozvrhu v rámci programu povědomí o bezpečnosti a školení (viz. kapitola 5.4.3).

Aby byla zajištěna neustálá vhodnost, přiměřenost a efektivnost politik, je důležité jejich **přezkoumávání v pravidelných intervalech**. Revize dokumentů je nutná i v případě, že v organizaci nastanou změny většího rozsahu. Odpovědnost za přezkoumávání nese management. Revize politik by měla zahrnovat také prostor pro zlepšení politik a přístupu k řízení bezpečnosti informací.

### 5.4.2 Organizace bezpečnosti informací

**Interní organizace**

**1) Role a odpovědnosti**

Za osobní zdravotní informace je zodpovědné vedení organizace. Pro řízení a koordinaci bezpečnosti informací se stanoví funkce. K těmto funkcím budou přiřazeny odpovědnosti:

- **představitel vedení** – dohlíží na provádění systému bezpečnosti informací, stanovuje politiku bezpečnosti informací, určuje role a jejich odpovědnosti, spolu s bezpečnostním manažerem a vlastníky aktiv definuje hodnocení aktiv, stanovuje hodnocení rizik,
- **manažer bezpečnosti** – odpovědný vedení společnosti za efektivní implementaci ISMS, tvorbu návrhů, bezpečnostních norem a směrnic, zajišťuje komunikaci s administrátorem, je zodpovědný za smlouvy a komunikaci s dodavateli, sleduje dodržování stanovených opatření a provádění jejich změn, zaznamenává změny a hlásí je představiteli vedení,

- **vlastníci aktiv** – každý vlastník je zodpovědný za přidělené aktivum, jsou dokumentovány podrobnosti k této odpovědnosti (seznam aktiv, jejich vlastníci, pravidla pro zacházení s přidělenými aktivy),
- **administrátor** – zodpovídá a provádí bezpečnostní opatření, komunikuje návrhy na technologické návrhy na bezpečnostní opatření s manažerem bezpečnosti a vedením, jeho úkolem je konfigurace hardware i software, zajištění připojení do sítě polikliniky, zajištění antivirové ochrany, nastavení elektronické pošty, případně i nákup nového hardware po konzultaci s vedením
- **auditor ISMS** – zaměstnanec organizace, který je povolán jako interní auditor.

**Odpovědnost za bezpečnost zdravotnických informací má v rámci organizace každý, kdo s těmito daty pracuje.**

Všechny technologické prostředky, které zpracovávají informace, se musí před jejich zavedením do provozu zkontrolovat, správně nastavit a schválit jejich nasazení v organizaci. Schvalovací proces má na starosti představitel vedení společnosti.

Administrátor dále zajistí, že:

a) všechny nové technologické prostředky musí být zkontrolovány a jsou kompatibilní s již zavedenými systémovými prvky,
b) zaměstnanci jsou povinni používat přidělené prostředky pouze k náplni své práce, zároveň projdou náležitým proškolením, jak s těmito zařízeními správně pracovat a jak dodržovat nastavená bezpečnostní opatření,
c) u každého nového prostředku dojde k posouzení, zda nebudou ovlivněna nastavená bezpečnostní opatření.

Problematiku bezpečnosti informací je třeba pravidelně projednávat. Tohoto jednání se účastní vedení společnosti a bezpečnostní manažer. Jednání stanoveného představenstva se koná alespoň 1x za čtvrt roku.

**2) Oddělení odpovědností**

Aby se zamezilo zneužití přístupu k aktivům ze strany interních zaměstnanců, je třeba oddělit odpovědnosti. Tímto se zamezí příležitosti neoprávněně nebo neúmyslně provést změny.

V analyzované organizaci by se toto pravidlo mělo zavést zejména při přihlašování do počítačů. Je doporučeno striktně přidělit každému zaměstnanci své osobní přihlašovací údaje a od zaměstnanců vyžadovat, aby je používali. Měl by být zaveden centralizovaný systém správy uživatelů ať lze jednoduše spravovat oprávnění zaměstnanců (především centrální odebrání přístupu odcházejícímu zaměstnanci). Toto opatření může pomoci tomu, že pokud se změní jakákoliv data ve zdravotnické dokumentaci nebo konfigurace počítačů, bude monitorováno, kdo byl v tuto dobu přihlášen. Pro přístup do konfigurace síťových prvků a serveru by měl mít pouze administrátor, popř. správce sítě, který je zaměstnán u polikliniky.

**3) Kontakt s autoritami**

Organizace by měla mít zavedené postupy, které určují, kdo a kdy může kontaktovat autority (orgány dohledu) a jakým způsobem je zajištěno včasné hlášení identifikovaných incidentů bezpečnosti informací.

**4) Kontakt se zvláštními zájmovými skupinami**

Pro organizaci může být velkým přínosem udržování přiměřených vztahů s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími. Prospěch vyplývá zejména z hlášení kybernetických bezpečnostních incidentů správním orgánům. Týká se to však i přístupu k informacím o nových technologiích, hrozbách či zranitelnostech. V kontextu analyzované společnosti spadá kontakt se skupinami do kompetence vedoucího lékaře (majitel společnosti) ve spolupráci s administrátorem (externí společnost).

**Práce na dálku**

V současnosti se v ambulanci nedá pracovat na dálku. Není ani možné využívat vlastních mobilních zařízení. V případě, že by se tento moderní způsob práce do organizace zaváděl, je nutné nastavit opatření i v této oblasti.

### 5.4.3 Bezpečnost lidských zdrojů

**Před vznikem pracovního poměru**

Před nástupem do pracovního poměru (hlavního či pouze brigádně) je důležité zaměstnancům vysvětlit jejich povinnosti. To stejné platí i pro smluvní strany.

1) **Prověřování**

   Organizace by měla před nástupem uchazeče do zaměstnání ověřit několik skutečností:

   - ověření životopisu žadatele (doložení diplomů a odborných kvalifikací),
   - ověření totožnosti (občanský průkaz, případně jiný doklad totožnosti),
   - podrobnější ověření (výpis z rejstříku trestů),
   - je-li to možné, ověření osobního posudku od bývalého zaměstnavatele.

   Je vhodné určit osobu, která se tímto ověřením bude zabývat. Důležité je kandidáty předem informovat o tomto ověření. Veškeré shromážděné údaje o uchazečích by měly být uchovávány dle platného zákona o nakládání s osobními údaji.

   Proces ověřování by měl být stanoven také pro smluvní strany.

2) **Podmínky pracovního poměru**

   Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat **ustanovení o** jejich **odpovědnostech** a o odpovědnostech organizace za bezpečnost informací. Všichni zaměstnanci a smluvní strany, kteří získávají přístup k aktivům organizace (zejména zdravotnická dokumentace) musí podepsat **smlouvu o mlčenlivosti**. Smlouvu je nutno podepsat dříve, než zaměstnanec dostane přístup k aktivům. Zároveň je doporučeno připojení **informace o právní odpovědnosti** za svěřená (zdravotnická) data. Dále je potřeba zaměstnance informovat o odpovědnosti

za správu přidělených aktiv. Podstatné je i sdělení o povinnostech ve vztahu k zacházení s informacemi získaných od jiných společností nebo externích subjektů.

Neméně důležitým dodatkem smlouvy má být výčet opatření přijatých v případě, že zaměstnanec ignoruje bezpečnostní požadavky organizace (sankce, příp. disciplinární řízení apod.). Zaměstnanci musí být o všech skutečnostech řádně informování a veškeré dokumenty je nezbytné opatřit podpisy.

V případě zaměstnanců ve zdravotnictví je navíc velmi podstatné neopomenout, že **zachování mlčenlivosti** je nutné dodržet i **po rozvázání pracovního poměru**.

**Během pracovního poměru**

**1) Odpovědnosti managementu organizace**

Management by měl požadovat od zaměstnanců i všech smluvních stran dodržování bezpečnosti informací v souladu se zavedenými politikami a postupy organizace. Jeho povinností je všechny zaměstnance informovat o jejich rolích a odpovědnostech v oblasti bezpečnosti informací ještě předtím, než dostanou k informacím přístup. Zaměstnanci musí obdržet přístup ke směrnicím a měli by být motivováni k plnění politiky bezpečnosti informací. Personál je třeba v této oblasti vzdělávat. Každý zaměstnanec má mít zpřístupněn anonymní kanál pro ohlašování porušení politik nebo postupů, z důvodu upozornění na protiprávní jednání. Stejné podmínky by měly platit i pro smluvní strany.

**Management musí** dát najevo podporu stanovených politik a **být vzorem**.

Pro efektivní řízení zdravotnických informačních systémů je třeba řešit také obavy některých pacientů, kteří si nepřejí, aby k jejich zdravotnickým údajům měli přístup konkrétní zdravotníci. Argumenty vychází zpravidla z narušených sousedských nebo příbuzenských vztahů.

### 2) Povědomí, vzdělávání a školení o bezpečnosti informací

Součástí ustavení politiky organizace je i **plán o školení a vzdělávání** zaměstnanců (případně i smluvních stran).

Program zvyšování povědomí o bezpečnosti by měl vypadat takto:

- ustaven v souladu s politikami organizace,
- bere v úvahu informace, které mají být chráněny,
- představuje opatření, která byla na ochranu informací zavedena,
- je pravidelně pořádaný,
- je postaven na poučení se z incidentů,
- je zaměřen nejen na faktory „co“, „jak“, ale i „proč“,
- vysvětluje pozitivní i negativní dopad zavedení bezpečnosti informací,
- je sestaven pro konkrétní role v organizaci (při nástupu, při povýšení atd.).

Nabízí se široká škála forem školení. Například samostudium, webový kurz či přednášky. Je vhodné zavést i další osvětové kampaně (informační brožury, pravidelný zpravodaj). Součástí pravidelně konaných kurzů by měl být vždy test porozumění nově nabytým znalostem.

### 3) Disciplinární řízení

Při nedodržování opatření, vedoucích k narušení bezpečnosti informací, by měl být zaveden **formální disciplinární proces**. Toto řízení bere v úvahu závažnost porušení. Rozlišuje, zda se jedná o první nebo opakovaný přestupek a zkoumá správnost proškolení narušitele. Disciplinární proces by měl odradit další zaměstnance od porušování bezpečnostních politik nebo motivovat ty, kteří na toto porušení upozorní, k získání mimořádného ocenění za dobrý počin.

**Ukončení a změna pracovního poměru**

**1) Odpovědnosti při ukončení nebo změně pracovního poměru**

Ve smlouvě o mlčenlivosti a v podmínkách pracovního poměru mají být zahrnuty **pokračující požadavky** na bezpečnost informací a právní odpovědnosti při ukončení pracovní smlouvy.

Jestliže zaměstnanec přechází na jinou pozici, je nezbytné podepsat **novou pracovní smlouvu** i nové podmínky pracovního poměru.

Přípravu nových smluv a dodatků obstarává externí účetní a personalistka. S touto externí společností je třeba **uzavřít dohodu o úrovni služeb** (SLA[23]), kde budou jasně definovány veškeré záležitosti.

### 5.4.4 Řízení aktiv

**Odpovědnost za aktiva**

**1) Seznam aktiv**

Organizace provede identifikaci aktiv a dokumentaci jejich významu. Zahrnout by se měl celý životní cyklus informací, tj. vytvoření, zpracování, ukládání, přenos, vymazání a zničení.

Aktiva, která byla identifikována na základě analýzy organizace, jsou uvedena v kapitole 5.1. **Seznam aktiv musí být stále aktuální**. Ke každému aktivu se stanoví vlastník a klasifikace (uvedeno v kapitole 5.1). Evidovat se musí každá změna a kontrola bude prováděna minimálně jednou za 2 roky.

**2) Vlastníci aktiv**

Ke každému aktivu bude přiřazen jeho vlastník. Vlastník ponese za aktiva odpovědnost a má povinnost je náležitě chránit. Je možné ustanovit jednotlivce nebo entitu. Určený vlastník nemusí mít nezbytně vlastnická práva k aktivu.

[23] SLA (z angl. Service Level Agreement)

O vedení zdravotnické dokumentace se sice stará vedoucí lékař, ale odpovědnost za ni ponesou všichni, kteří mají přístup.

U papírové zdravotnické dokumentace, která je uložena v archivu polikliniky, bude potřeba zajistit správné nakládání v souladu s bezpečnostní politikou organizace, a to prostřednictvím smlouvy SLA.

**3) Používání aktiv**

K identifikovaným a dokumentovaným aktivům mají být zároveň přidělena pravidla pro přípustné používání. Je potřeba uvědomit také externí strany mající přístup k aktivům (např. administrátor k zálohám na serveru či k elektronické dokumentaci v informačním systému) o požadavcích bezpečnosti informací. V této souvislosti bude nezbytné zajistit spolupráci s externími dodavateli pomocí smluv SLA a smlouvy o mlčenlivosti.

**4) Vrácení aktiv**

Po ukončení zaměstnání, smlouvy nebo dohody musí všichni zaměstnanci a uživatelé externích stran vrátit všechna aktiva, která spravovali. Administrátor je povinen zajistit, že odebere přístupová práva zaměstnance.

## Klasifikace informací

1) Klasifikace informací

Všechny informace, které má organizace k dispozici, budou klasifikovány tímto způsobem:

- **Interní informace** – jsou informace, které vznikly z činnosti firmy nebo s její činností souvisejí. Jejich vyzrazení, zneužití nebo poškození může být pro organizaci nevýhodné. Interní informace se nijak specificky neoznačují a může s nimi být manipulováno v rámci firmy bez rozlišení zaměstnanců.
- **Důvěrné informace** – jsou informace, které vznikly činností firmy. Jejich vyzrazením, poškozením nebo zneužitím může být vážně poškozeno dobré

jméno organizace. Tyto informace je třeba rozlišovat značkou „důvěrné“ a mohou s nimi manipulovat pouze osoby, které to mají v popisu práce.

Klasifikace informací jednoznačně určuje, jak s nimi zacházet a chránit je.

**2) Označování informací**

Informací se pro potřeby této směrnice rozumí dokumenty v elektronické i listinné formě. V elektronické formě se může jednat o zdravotnické záznamy v podobě textu, snímku či videa.

Při vzniku informace nebo při přijetí informace od externí strany určí zaměstnanec její klasifikační stupeň. Vznik zdravotnické dokumentace nebo příjem laboratorních výsledků bude vždy klasifikováno jako „důvěrné“. Zaměstnanec odpovídá za bezpečné uložení této informace. Zaměstnanec viditelně označí dokument nebo datový nosič nálepkou či nápisem na první stranu nebo obal datového nosiče.

**3) Manipulace s aktivy**

Dokumenty označené klasifikací „důvěrné“ je potřeba bezpečně uschovat. Dokumentace v listinné podobě musí být uzamčena v kartotéce nebo v trezoru. Elektronické dokumenty musí být přístupné pouze po zadání přístupového hesla do počítače nebo informačního systému. U dokumentů mimo ordinaci je nutné zabezpečení dle této směrnice. K tomu je zapotřebí podepsat smlouvy SLA s externími stranami.

V případě zasílání informací je nezbytné dodržovat tyto postupy:

- listinná dokumentace (karty pacientů, laboratorní výsledky, žádanky) se zasílá prostřednictvím kurýra nebo doporučené pošty,
- elektronická dokumentace je odesílána výhradně prostřednictvím zřízené (a zabezpečené) e-mailové schránky,
- elektronické dokumenty se ukládají do .ZIP souborů s nastavením unikátního hesla,
- heslo se neposílá ve stejném e-mailu jako dokumentace, ale sdělování probíhá prostřednictví telefonu nebo osobně,

- sdělení hesla po telefonu se provádí až po ověření, že u telefonu je správný příjemce (např. pomocí bezchybného uvedení rodného čísla).

V případě, dokumentu určeného k vyřazení, jej nelze vložit do koše, ale je nutná skartace za použití skartačního přístroje.

**Manipulace s médii**

1) **Správa výměnných médií**

Pro správu výměnných médií by měly být zavedeny postupy v souladu se schématem klasifikace přijatým organizací. Datové nosiče se označují stejným způsobem, jako dokumenty v listinné formě. S médii musí být nakládáno tak, jak určuje výrobce, aby nedošlo k jejich nechtěnému zničení dat. Z médií, která lze opakovaně použít, musí být původní obsah nenávratně vymazán.

2) **Likvidace médií**

Nepotřebná média je nutné zlikvidovat např. skartováním nebo vymazáním důležitých údajů.

3) **Přeprava fyzických médií**

Pokud je nezbytné média zasílat mimo organizaci, platí stejný řád, jako pro zasílání listinných dokumentů.

**Únik informací klasifikačního stupně „důvěrné“ je považováno za incident bezpečnosti informací.**

### 5.4.5 Řízení přístupu

**Požadavky organizace na řízení přístupu**

**1) Politika řízení přístupu**

Politika řízení přístupu stanovuje přístup k informacím a zařízením pro zpracování informací. Tato politika musí být vytvořena, dokumentována a přezkoumávána.

Je důležité stanovit pravidla na základě principu „*Všechno, co není výslovně povoleno, je zakázáno*“.

**Správa a řízení přístupu uživatelů**

**1) Registrace a zrušení uživatele**

Pro přidělování přístupových práv se zavede postup formální registrace, kterou technologicky zajistí administrátor. Důležité je, aby administrátor používal jedinečné ID uživatele, odstraňoval průběžně duplicity. V případě odchodu zaměstnance z organizace zrušil okamžitě jeho přístupová práva.

**2) Zřízení přístupu uživatele**

Měl by být zaveden formální postup pro přiřazení přístupových práv pro všechny typy uživatelů. O přidělení přístupových práv je nutné vést centrální evidenci. Pozornost musí být věnována i doložkám pracovních a dodavatelských smluv, ve kterých jsou specifikovány sankce v případě, že dojde k pokusu o neoprávněný přístup.

**3) Řízení privilegovaných přístupových práv**

Použití privilegovaných přístupových práv musí být omezeno a řízeno. Přidělení speciálních přístupů je důležité předem zvážit, důsledně dokumentovat a pravidelně přezkoumávat.

**4) Přezkoumání přístupových práv**

Při každé změně, jako je přestup na vyšší pozici nebo odchod ze zaměstnání, by měly být přístupová práva přezkoumávána. Autorizace pro privilegovaná práva je doporučeno přezkoumávat častěji. Veškerá dokumentace, ve které jsou přístupová práva zaznamenána, musí reflektovat na tyto změny a měla by se upravovat zároveň se změnou přístupů.

### 5) Odebrání nebo úprava přístupových práv

Přístupová práva by měla být odebrána ihned po ukončení pracovního poměru nebo při vypršení smlouvy. Úprava v důsledku změny pracovní pozice musí proběhnout taktéž neprodleně. Tato práva zahrnují fyzický i logický přístup.

Zvýšená pozornost je důležité věnovat v případě, že zaměstnanec opouští pracovní místo v důsledku nespokojenosti nebo z iniciativy managementu.

## Odpovědnosti uživatelů

### 1) Použití tajných autentizačních informací

Všichni uživatelé by měli být poučeni, aby:

- nevyzrazovali hesla žádným jiným stranám, včetně úředních osob,
- neměli hesla zapsaná např. na papíře nebo v souboru,
- změnili heslo kdykoliv se vyskytne náznak její možné kompromitace,
- volili kvalitní hesla s minimální dostatečnou délkou,
- neukládali hesla v automatizovaných přístupech,
- **nepoužívali stejná hesla pro různé účely**.

Sestavení tajných autentizačních informací:

- heslo není lehce zapamatovatelné,
- nejsou snadno uhodnutelná (jména, data narození atd.),
- nejsou zranitelná slovníkovými útoky,
- neobsahují po sobě jdoucí znaky,
- jsou-li dočasná, musí být změněna po prvním přihlášení.

## Řízení přístupu k systémům a aplikacím

### 1) Omezení přístupu k informacím

Přístup k systémům a aplikacím by měl být omezen v souladu s politikou řízení přístupu. Je potřebné, aby docházelo k pravidelné kontrole přístupů uživatelů k různým datům. Zároveň se doporučuje kontrolovat i přístupová práva uživatelů, např. práva číst, psát, mazat a vykonávat. V nutných případech může být zavedeno i omezení informací obsažených ve výstupech.

### 2) Bezpečné postupy přihlášení

V souladu s politikou přístupu by měl být definován bezpečný postup přihlášení. Pro přihlašování k jednotlivým počítačům se musí použít oddělené účty, které jsou zabezpečeny heslem. Pro přístup ke zdravotnickým datům v informačním systému je vyžadován přístup pomocí ID a hesla. Každý uživatel má povinnost používat svůj přiřazený e-mailový účet. Při startu informačního systému je účelné zobrazování hlášky, že informace obsažené v systému, jsou důvěrné.

Model správného postupu přihlášení:

- nezobrazují se identifikátory aplikace, dokud není proces přihlášení úspěšně dokončen,
- zobrazuje se varovné upozornění, že přístup by měli mít jen oprávnění uživatelé,
- během přihlašovací procedury se nezobrazují žádné pomocné hlášky, které by dopomohly neoprávněnému uživateli,
- v případě chybového stavu hlášení systému, že zadaná data jsou nesprávná,
- chránit před pokusy o přihlášení hrubou silou,
- zaznamenávají se úspěšné i neúspěšné pokusy formou logů,
- nezobrazuje se zadávané heslo,
- neaktivní relace se samy ukončují.

3) **Systém správy hesel**

Systém správy hesel by měl:

- vynutit použití ID a hesla pro přihlášení,
- umožnit uživateli výběr a změnu hesla,
- vynutit výběr kvalitních hesel,
- vynutit pravidelné změny hesla,
- zabraňovat opětovnému použití hesel,
- nezobrazovat hesla na obrazovce,
- ukládat soubory s hesly odděleně od dat aplikačních systémů.

Použití správného a funkčního systému správy hesel by měl vynutit administrátor po odsouhlasení těchto postupů managementem.

### 5.4.6 Fyzická bezpečnost a bezpečnost prostředí

**Zabezpečené oblasti**

1) **Fyzický bezpečnostní perimetr**

Fyzický bezpečnostní perimetr by měl být jasně definován. Bezpečnostní perimetr nesmí mít žádná místa, kudy lze snadno proniknout (např. nevhodně chráněné vnější dveře, otevřená okna v době nepřítomnosti). Vhodné disponovat recepcí, což organizace v současnosti splňuje. Požární dveře musí být zajištěny dle požárních předpisů a norem. O zajištění prostor polikliniky se stará ostraha pomocí kamerového systému a dalších opatření, které jsou popsány v analýze společnosti.

2) **Fyzické kontroly vstupu**

V ordinační dny se do prostor ambulance dostanou pouze pacienti a zaměstnanci přes recepci. Přístup do čekárny je volný. V době nepřítomnosti je nutné vstupní dveře zamykat a před odchodem také zkontrolovat úplné zavření všech oken. Možnost má po ukončení ordinační doby jen uklízečka, příp. ostraha. Tyto osoby je nutné poučit ohledně bezpečnostních požadavků. Bylo by vhodné **zprovoznit systém pro kontrolu příchodu a odchodu zaměstnanců,** který zaznamenává, kdo a v kolik

hodin se v prostorech ambulance nacházel. Vhodným doplňkem může být **čipový systém** umístněný před vstupními dveřmi. Čipové karty pak vlastní pouze zdravotnický personál, lékaři, úklidová služba a ostraha. Přístupová práva (tzn. vrácení klíčů a čipových karet) musí být neustále přezkoumávána a odebírána v případě, že zaměstnanec ukončil pracovní smlouvu.

Vhodné ke zvážení je i umístění **kamery se záznamem** ke vstupním dveřím. Neboť kamerový systém polikliniky nehlídá vstupy k jednotlivým ordinacím, ale pouze chodby, vstupy do budovy a parkoviště.

**3) Zabezpečení kanceláří, místností a vybavení**

Klíče od jednotlivých ordinací, případně jakékoliv další, je vhodné uschovat, aby se zabránilo přístupu veřejnosti. Je nevhodné viditelné dražšího vybavení z důvodu přilákání pozornosti.

Dveře propojující ordinace lékařů se sesternou jsou protihlukově zabezpečeny polstrováním.

**4) Ochrana před vnějšími a přírodními hrozbami**

Jelikož se budova polikliniky nachází v blízkosti velkého říčního toku, předpokládá se, že zabezpečení proti povodním řeší správa polikliniky. Stejným způsobem musí být ošetřeno i protipožární opatření dle platných norem a vyhlášek.

**Zařízení**

1) Umístění zařízení a jeho ochrana

Pro **zamezení sledování obrazovek** od počítačů neoprávněnými osobami by se mělo zvážit jejich správné umístění ve všech prostorách ambulance. Při odchodu pacienta z ordinace je důležité zavírat jeho kartu, aby nedošlo ke čtení zdravotnických údajů jinými osobami. Pokud personál od počítače odchází, je nutné jej zamykat. Média pro ukládání dat (např. flash disky) by měla být bezpečně uschována v uzamykatelné zásuvce.

**Do kartotéky** pro papírovou zdravotnickou dokumentaci je nezbytné **nainstalovat zámky**. Lednici s očkovacími látkami může personál otevřít pouze za použití klíče. Klíč je nutné uschovat spolu s dalšími na bezpečné místo.

V ordinaci je udržována stálá teplota pomocí klimatizace a ústředního topení. Udržování stálé teploty je podstatné zejména pro zařízení, která mají dané určité teplotní limity, při kterých je zaručena správná funkčnost.

**2) Podpůrné služby**

Veškeré zásobování energiemi a vodou zajišťuje poliklinika. Předpokládá se, že správa budovy má zavedené ochrany proti výpadkům a dalším poruchám. Ordinace by měla mít dostupnost těchto služeb uvedenou ve smlouvě SLA. Nouzové osvětlení a východy má v kompetenci taktéž poliklinika.

V ambulanci jsou všechny počítače včetně serveru napojeny na zdroj nepřerušovaného napájení, což zabrání případným problémům např. při ukládání dat. Tyto záložní zdroje navíc obsahují baterii, která poskytne napájení dalších cca 20 minut pro počítače při výpadku elektrického proudu.

Do ambulance se nakupují pouze ta zařízení, která mají požadovanou technickou shodu a je povolen jejich prodej v rámci zemí EU.

**3) Bezpečnost kabelových rozvodů**

Silová i telefonní kabeláž by měla být chráněna před odposloucháváním, rušením a poškozením. Toto opatření má na starosti poliklinika a předpokládá se správné zabezpečení ze strany polikliniky.

Za bezchybné zapojení a položení kabeláže přímo v ambulanci zodpovídá správce objektu, který je zaměstnancem polikliniky. Dodržovat správné zapojení musí také administrátor, který se stará o nákup hardware a software do organizace. Důležité je oddělení komunikačních kabelů od napájecích, aby nedocházelo k rušení.

V pravidelných intervalech musí docházet ke kontrole kabeláže, zda není poškozená a není třeba ji vyměnit za novou. Toto má v kompetenci administrátor, který vede také aktuální schéma zapojení.

**4) Údržba zařízení**

Administrátor zajistí, že:

- provedení oprav provádí pouze autorizovaný servis nebo autorizovaní pracovníci údržby,
- je veden provozní deník o provedených opravách, údržbě a kontrolách,
- zařízení IT, na kterém jsou ukládány důvěrné informace, je zasíláno do opravy jen po vyjmutí disku nebo po spolehlivém odstranění dat ze zařízení.

**5) Bezpečnost zařízení a aktiv mimo prostory organizace**

Aktiva, která se nachází mimo gynekologickou ambulanci jsou[24]:

- personální a účetní data,
- archivovaná zdravotnická dokumentace,
- originál dokumentace ISO 9001,
- dodavatelské smlouvy.

Předpokládá se správné nakládání se jmenovanými aktivy. Pro zajištění, že tomu tak opravdu bude, se sestaví smlouvy SLA.

**6) Bezpečná likvidace nebo opakované použití zařízení**

Před likvidací nebo znovupoužitím zařízení IT, na nichž byly zpracovávány informace, se provede bezpečné smazání těchto informací. Za likvidaci zařízení využívaného pro manipulaci neveřejných informací bude odpovídat administrátor.

**7) Neobsluhovaná uživatelská zařízení**

Všichni uživatelé by měli být informováni o bezpečnostních požadavcích a postupech pro ochranu neobsluhovaného zařízení, jakož i o jejich odpovědnosti za realizaci této ochrany. Nutné požadavky:

- uzamčení počítače, pokud se od něj uživatel vzdaluje,
- po ukončení pracovní doby se odhlásit z informačního systému, e-mailu a dalších aplikací,

[24] Kompletní seznam všech aktiv je k nalezení v kapitole 5.1.

- po ukončení pracovní doby uzamknout počítač.

**8) Zásada prázdného stolu a prázdné obrazovky monitoru**

Zásada spočívá v těchto bodech:

- důvěrné informace v papírové formě (nebo na paměťovém médiu) by měly být uzamčeny, pokud nejsou využívány,
- počítače jsou ponechány s odhlášenými uživateli,
- média obsahující důvěrné informace mají být ihned odebrány z tiskáren.

### 5.4.7 Bezpečnost provozu

**Provozní postupy a odpovědnosti**

**1) Dokumentace provozních postupů**

Měly by být vypracovány postupy pro zapnutí/vypnutí počítače, zálohování, údržbu zařízení, zacházení s médii, zacházení s poštou a bezpečnost práce.

Provozní postupy je třeba vypracovat formálně a změny musí schválit management. Tyto postupy jsou již formulovány v dokumentaci ISO 9001, která je k dispozici všem zaměstnancům, kteří se jí řídí.

**2) Řízení změn**

Veškeré změny v organizaci, podnikových procesech, vybavení pro zpracování informací a systémech, které mají vliv na bezpečnost informací, by měly být řízeny a dokumentovány. Vždy se musí znovu posuzovat dopad těchto změn na bezpečnost informací. Je doporučeno zavést formální postup pro schvalování změn. Na závěr se musí ověřit, zda jsou i nadále splněny požadavky na bezpečnost informací.

**Ochrana před malware**

**1) Opatření na ochranu proti malware**

Je třeba zvážit tato opatření:

- zákaz instalace neautorizovaného softwaru,
- znemožnění otevírání podezřelých webových stránek,

- stanovení formální politiky na ochranu proti rizikům spojených se získáním dat z internetu nebo přenosových médií,
- pravidelná aktualizace software pro detekci proti malware,
- definovat postupy a odpovědnosti zabývajících se ochranou před malware,
- pravidelné školení uživatelů,
- pravidelné skenování počítačů (soubory stažené z internetu, e-mailové přílohy),
- připravit plány na zotavení po útoku vyvolaném malware.

**Použití samotného softwaru na detekci malware není obvykle dostačující a často musí být doprovázeno provozními postupy, které brání zavedení malware.**

Počítače na ambulanci by měly být dále chráněny personálním firewallem. Pro komunikaci pomocí elektronické pošty je účelné nasadit centrální on-line antivirový software s nastavením antispamových pravidel na poštovním serveru a automatickou aktualizací.

**Zálohování**

1) **Zálohování informací**

Zálohování zdravotnických dat a obrazu pevného disku by mělo být doplněno konfigurací pro zvýšení spolehlivosti systému (RAID[25]). Zálohy uložené na serveru by dále měly být šifrovány, aby se k nim nedostaly nepovolané osoby.

**Zaznamenávání formou logů a monitorování**

1) **Zaznamenávání událostí formou logů**

Měly by být pořizovány, uchovávány a pravidelně přezkoumávány záznamy událostí formou logů, které zaznamenávají aktivitu uživatelů či různá selhání. Logovací systém by měl sbírat tyto záznamy:

[25] RAID (z angl. Redundant Array of Independent Disks)

- ID uživatele,
- datum a čas přihlášení/odhlášení,
- použité aplikace a nástroje,
- soubory, ke kterým bylo přistupováno.

Administrátor by neměl mít oprávnění vymazat nebo deaktivovat záznamy formou logů o svých vlastních aktivitách.

Samotné záznamy musí být chráněny proti falšování a neoprávněnému přístupu.

Pro zajištění správné funkcionality systému pro sběr logů je důležité nastavení správného času.

**Správa a řízení technických zranitelností**

1) **Správa a řízení technických zranitelností**

   Je podstatné, aby organizace využívala informační systém, který je odolný proti zranitelnosti. Tomu se dá zabránit zejména pravidelnou aktualizací. Sledovat se musí také to, zda dodavatel nepřestal některou z dříve vydaných verzí podporovat.

   Ambulance by měla zkontrolovat aktuálnost software a informačního systému a zajistit případnou aktualizaci nebo přechod na zcela novou verzi.

   V případě, že dojde k podezření na technickou zranitelnost, je nezbytné ihned reagovat a nechat si systém záplatovat. Veškeré změny (aktualizace, nová verze) je třeba zaznamenat do seznamu změn a management musí změnu schválit.

2) **Omezení instalace softwaru**

   Administrátor by měl zajistit, aby na počítačích v ambulanci byla omezena instalace dalšího software. Aktualizace všech instalovaných programů by se měla nastavit tak, aby se prováděla automaticky.

### 5.4.8 Bezpečnost komunikací

**Správa bezpečnosti sítě**

Ve smlouvě o síťových službách (mezi ambulancí a poliklinikou) by měly být zahrnuty požadavky na úroveň služeb a na správu a řízení všech síťových služeb.

Veškerá síťová nastavení má na starosti správce sítě, který je zaměstnán u polikliniky. Zachování oddělené sítě ambulance od polikliniky je vhodné a zachová se nadále.

**Přenos informací**

1) Politiky a postupy při přenosu informací

Měly by být definovány tyto postupy:

- ochrana přenášených informací před odposloucháváním, kopírováním, pozměněním, chybným směrováním a zničením,
- detekce a ochrana malware, který může být přenesen pomocí elektronické komunikace,
- ochrana důvěrných informací, které jsou odesílány v příloze e-mailu,
- odpovědnosti zaměstnanců za pomluvy, obtěžování, přeposílání řetězové pošty, neoprávněné nakupování,
- směrnice o uchování a likvidaci podnikové korespondence,
- doporučení zaměstnancům o přijetí vhodných opatření proti prozrazení důvěrných informací.

Sdělování důvěrných informací prostřednictvím telefonního rozhovoru nesmí být vedeno v otevřených místnostech nebo před dalšími pacienty.

**2) Elektronické předávání zpráv**

Při předávání informací pomocí elektronické pošty nebo skrze informační systém (formuláře pro pojišťovny) musí uživatel pečlivě kontrolovat správné adresování zprávy. Používání jakékoliv jiné služby je zakázáno (zejména sociální sítě či veřejná datová úložiště).

E-mailová komunikace by měla být chráněna před neoprávněným přístupem, změnou nebo odmítnutím služby. Zároveň musí být dodržována zákonná kritéria ohledně požadavků na elektronické podpisy.

**3) Dohody o důvěrnosti nebo mlčenlivosti**

K dohodám o mlčenlivosti, které je povinen každý zaměstnanec při nástupu podepsat, by měla být připojena informace o sankcích v případě porušení dohody.

### 5.4.9 Akvizice, vývoj a údržba systému

**Bezpečnostní požadavky informačních systémů**

**1) Analýza a specifikace požadavků bezpečnosti informací**

Informační systémy zahrnují operační systémy, infrastrukturu, specializované aplikace a komerční programové produkty. Bezpečnostní požadavky musí být identifikovány a schváleny před pořízením, změnou nebo implementací. V rámci vývoje a údržby informačních systémů musí být do životního cyklu IS prosazena, počínaje návrhem změny, základní bezpečnostní opatření předcházející ztrátě, modifikaci a zneužití informací.

V rámci správy provozního programového vybavení se musí dodržovat následující zásady:

a) změny a aktualizace programového vybavení smí provádět pouze oprávněná osoba dle stanovených postupů popsaných dodavatelem programového vybavení,

b) veškeré změny provozního programového vybavení musí být zaznamenány.

Zdravotnické informační systémy musí zaručit jednoznačnou identifikaci pacienta.

**2) Zabezpečení aplikačních služeb ve veřejných sítích**

Přístup do databáze laboratoří by měl probíhat výhradně za použití autentizačních údajů. Požadovaná úroveň důvěry musí být splněna pro obě strany. Dohodu mezi partnery o aplikačních službách je vhodné podepřít zdokumentovaným souhlasem, který zavazuje obě strany k dohodnutým podmínkám služeb.

### 5.4.10 Vztahy s dodavateli

**Bezpečnost informací ve vztazích s dodavateli**

1) **Bezpečnosti informací pro oblast vztahů s dodavateli**

V organizaci by měla být definována politika pro řízení vztahů s dodavateli, kde jsou určena opatření, kterými se dodavatelé musí řídit. V politice by měl být veden seznam dodavatelů. Lze vycházet ze seznamu dodavatelů uvedených v dokumentaci ISO 9001. Soupis musí obsahovat definice, k jakým datům má dodavatel přístup. Dále by mělo být uvedeno, jak bude monitorováno dodržování stanovených požadavků.

U dodavatelů, majících přístup do IT vybavení (tzn. i k e-mailům, případně do informačního systému) a ke zdravotnickým datům, je třeba **podepsat smlouvu o mlčenlivosti**.

2) **Řešení bezpečnosti v rámci smluv s dodavateli**

Měly by být ustaveny smlouvy s dodavateli, aby bylo dokumentováno, že nedošlo k žádnému nedorozumění mezi oběma stranami.

Obsahem smluv by mělo být:

- popis informací, které jsou dodavateli přístupné,
- právní a předpisové požadavky,
- povinnost každé strany zavést dohodnutý soubor opatření,
- pravidla akceptovatelného použití informací,
- seznam pracovníků, kteří budou mít přístup k informacím,
- politiky bezpečnosti informací týkající se konkrétní smlouvy,
- požadavky na řízení incidentů,
- požadavky na školení,
- právo provést audit procesů a opatření dodavatele souvisejících se smlouvou,
- postup řešení vad a konfliktů,
- povinnost dodavatele dodržovat bezpečnostní požadavky organizace.

Smlouvy s dodavateli musí zahrnovat požadavky na řešení rizik v oblasti bezpečnosti informací. Ve smlouvách by dále měly být definovány požadavky týkající se pořizování

produktů nebo služeb IT. Dodavatelé by zároveň měli propagovat bezpečnostní požadavky organizace také pro subdodavatele.

Organizace potřebuje mít jistotu, že lze vysledovat kritické komponenty a jejich původ a že dodané produkty a služby fungují dle očekávání.

**Řízení dodávky služeb dodavatelem**

1) **Monitorování a přezkoumávání služeb dodavatelů**

Organizace by měla sledovat dodržování smluv, provádět audity dodavatelů. Odpovědnost za řízení dodavatelských vztahů má bezpečnostní manažer. Pokud by byly shledány nedostatky v dodržování bezpečnosti informací, je třeba učinit příslušné kroky. Bezpečnostní manažer musí mít přehled o dodavatelích a jejich přístupech k důvěrným informacím.

2) **Řízení změn služeb dodavatelů**

Změny dodavatelů musí být řízeny a jejich schvalování je v kompetenci managementu.

Součástí řízení změn jsou také změny dodavatelských smluv, případně zlepšení dodavatelských služeb. Zahrnují se sem i úpravy a aktualizace politik a postupů organizace nebo nová opatření pro řešení incidentů a zdokonalování bezpečnosti.

Změny ze strany dodavatele musí být také monitorovány. Patří k nim používání nových technologií a produktů, nových verzí/vydání a subdodávky od jiného dodavatele.

### 5.4.11 Řízení incidentů bezpečnosti informací

**Řízení incidentů bezpečnosti informací a zlepšování**

1) **Odpovědnosti a postupy**

Měly by být stanoveny odpovědnosti a postupy managementu s cílem zajistit rychlou, efektivní a řádnou odezvu na incidenty bezpečnosti informací. Cílem správy incidentů

bezpečnosti informací je zajistit, aby incidenty a slabiny bezpečnosti informací byly komunikovány způsobem, který umožní včasnou nápravu s využitím formalizovaného a obecně známého postupu. Cíle pro řízení incidentů musí být schváleny managementem. Důležité je zajištění, že osoby, které mají řízení incidentů na starosti, rozumí prioritám organizace.

Pokud incidenty přichází globálně, měla by se informace o incidentu sdílet s externími organizacemi.

**2) Podávání zpráv o událostech bezpečnosti informací**

Kontaktní osoba pro hlášení incidentů je bezpečnostní manažer.

Všichni zaměstnanci a smluvní strany musí incidenty hlásit tak rychle, jak je to možné. Zaměstnanci by měli být seznámeni o postupu, jak incident ohlásit a na koho se v takovém případě obrátit. Hlásit je třeba každé neočekávané narušení integrity, důvěrnosti a dostupnosti informací. Do incidentů spadají také lidské chyby, špatná funkce softwaru a hardwaru nebo prolomení opatření fyzické bezpečnosti.

Organizace by měla informovat pacienta v případě, že došlo k neúmyslnému vyzrazení jeho osobních zdravotních informací.

**3) Podávání zpráv o slabých místech bezpečnosti informací**

Zaměstnanci jsou rovněž povinni upozornit a ohlásit podezření na slabiny systému nebo služeb. Oznámení by mělo proběhnout co nejrychleji, aby se zamezilo případnému incidentu bezpečnosti informací. Mechanismus podávání zpráv musí být snadný a přístupný. Zaměstnanci mají být poučeni o tom, že slabá místa nesmí prokazovat testováním. Tuto činnost je možné interpretovat jako zneužití systému. Mohlo by způsobit vážné poškození informačního systému nebo služby či vést k právní odpovědnosti jednotlivce provádějícího testy.

**4) Posuzování a rozhodování o událostech bezpečnosti informací**

Na kontaktním místě je navrženo posuzování každého oznámení. Následuje rozhodnutí, zda se jedná o bezpečnostní incident, či nikoliv. Incident musí být klasifikován a je nezbytné stanovit priority incidentů. To může dopomoci k určení

dopadu a rozsahu incidentu. Výsledky posouzení se zaznamenávají za účelem budoucí reference a ověření.

**5) Odezva na incidenty bezpečnosti informací**

Na incidenty bezpečnosti informací musí navazovat reakce. Odezva by měla obsahovat shromáždění důkazů a provedení analýzy. Dále oznámení existence incidentu dalším interním i externím stranám, které by měly být informovány. Ve fázi úspěšného vypořádání se s incidentem probíhá jeho uzavření a zaznamenání.

**Ponaučení z incidentů bezpečnosti informací**

Pro snížení pravděpodobnosti a dopadu budoucích incidentů by měly být zavedeny mechanismy, ve kterých bude možné najít řešení opakujících se incidentů.

Vyhodnocení incidentů by mělo vést k přezkoumání bezpečnostní politiky a k zavedení dalších opatření, aby se incident neopakoval. Příběhy skutečných incidentů mohou navíc posloužit při školení povědomí uživatelů.

### 5.4.12 Aspekty řízení kontinuity činnosti organizace

**Kontinuita bezpečnosti informací**

**1) Plánování kontinuity bezpečnosti informací**

Zachycení aspektů bezpečnosti informací v rámci obvyklé analýzy dopadů řízení kontinuity činností organizace nebo řízení obnovy po havárii snižuje čas a úsilí v případě další analýzy dopadu pro bezpečnost informací.

**2) Implementace kontinuity bezpečnosti informací**

Organizace by měla zajistit, že:

- je zavedena struktura řízení připravená na rušivé události,
- jsou jmenování pracovníci zabývající se odezvou na incidenty,
- jsou vypracovány plány a postupy odezvy a obnovy, které popisují, jak bude organizace udržovat svoji bezpečnost informací.

Tyto plány a postupy je vhodné vytvořit spolu se specialistou na bezpečnost, aby se docílilo toho, že pokud nebudou fungovat zavedená opatření, je nutné zavést jiná opatření, která bezpečnost informací zajistí.

**3) Verifikace, přezkoumávání a vyhodnocení kontinuity bezpečnosti informací**

Organizace by měla v pravidelných intervalech ověřit, zda jsou navržené plány a opatření kontinuity funkční i za nepříznivých situací.

### 5.4.13 Soulad s požadavky

**Soulad se zákonnými a smluvními požadavky**

**1) Identifikace příslušné legislativy a smluvních požadavků**

Management musí identifikovat, dokumentovat a udržovat všechny zákonné, předpisové, smluvní požadavky a přístup organizace ke splnění těchto požadavků. Ke splnění požadavků musí být specifikována další opatření a individuální odpovědnosti.

**2) Práva k duševnímu vlastnictví**

Pro ochranu subjektu, by měly být zváženy následující pokyny:

- zveřejnění politiky v souladu s právy duševního vlastnictví, kde je stanoveno legální použití softwaru,
- nákup softwaru pouze u ověřených zdrojů, aby nebylo porušeno autorské právo,
- udržování seznamu aktiv a identifikace všech aktiv s požadavky na ochranu práv duševního vlastnictví,
- uchovávání dokladů o vlastnictví licencí, manuálů apod.,
- sledovat překročení maximálního počtu uživatelů povolených v rámci licence,
- přezkoumávání, zda je instalován pouze autorizovaný software,
- stanovení politik pro likvidaci softwaru,
- nevytváření duplikátů nebo kopií (audio, video, kopie knih, článků apod.).

### 3) Ochrana záznamů

Při rozhodování o ochraně konkrétních záznamů organizace by měla být vzata v úvahu jejich odpovídající klasifikace vycházející z klasifikačního schématu organizace. Záznamy je vhodné roztřídit dle typu a měla by být přidělena doba uchování. Věnovat pozornost je nutné i skladovacím a manipulačním postupům (např. dle výrobce), aby nedocházelo ke zhoršení kvality záznamů (typicky u CD/DVD nosičů).

Archiv zdravotnických záznamů je umístěn v budově polikliniky. Nakládání s těmito dokumenty je ošetřeno ve smlouvě SLA. V případě personálních a účetnických dat je rovněž způsob skladování záznamů definován ve smlouvě.

Zákony a předpisy často stanovují, po jakou dobu musí být konkrétní dokumenty skladovány. Tyto záznamy je nutné uchovávat po celou dobu, která je určena. V případě kontrolního auditu od správních orgánů je nutné tyto dokumenty doložit.

### 4) Soukromí a ochrana osobních údajů

Zaměstnanci se při zabezpečení ochrany osobních údajů řídí zejména zákonem č. 101/2001 Sb., o ochraně osobních údajů ve znění pozdějších předpisů. Organizace by měly spravovat informační souhlas pacientů.

## Přezkoumání bezpečnosti informací

### 1) Nezávislé přezkoumání bezpečnosti informací

Pro zajištění neustálé vhodnosti, přiměřenosti a účinnosti musí management iniciovat nezávislé přezkoumání. Po přezkoumání by měly být posouzeny možnosti zlepšení. Přezkoumání bude prováděno nezávislým interním auditorem.

Pokud jsou po přezkoumání zjištěny nedostatky, měl by management zvážit nápravná opatření.

### 2) Soulad s bezpečnostními politikami a normami

Porovnání shody bezpečnostních norem se provede formou auditu ISMS. Pokud je nalezen jakýkoliv nesoulad, provede bezpečnostní manažer nápravná opatření:

- identifikuje příčinu nesouladu,
- vyhodnotí potřebné kroky k dosažení shody,
- implementuje opatření,
- přezkoumá nápravné opatření.

Výsledky přezkoumání a nápravných opatření by měly být zaznamenány a tyto záznamy uchovány.

**3) Přezkoumávání technického souladu**

Přezkoumání technického souladu zahrnuje posouzení operačních systémů k zajištění, že hardwarová a softwarová opatření byla správně implementována. Takové přezkoumání by měl provádět pouze auditor s technickými znalostmi. Testování může zahrnovat penetrační testy nebo posouzení zranitelností. Toto může sloužit pro kontrolu, že jsou opatření správně nastavena a pro odhalení zranitelností, na které je třeba se znovu zaměřit.

# 6 Zhodnocení a přínosy práce

Vypracovaná bezpečnostní příručka může posloužit jako návod při zavádění ISMS do analyzované organizace.

Zavedení a případná certifikace systému managementu bezpečnosti informací však není otázka několika hodin nebo dní. Nejprve je nutné vybrat odborníky, kteří se touto problematikou zabývají. Zvolený konzultant poté společně s managementem provádí potřebné kroky k přípravě auditu. Přichystání a zavedení opatření zaberou čas v řádech několika týdnů až měsíců (dle rozsahu ISMS). Samotná certifikace probíhá, dle velikosti firmy, kolem jednoho dne až celého týdne.

Investice do opatření a nápravných opatření po přezkoumání se pohybuje v řádech desetitisíců až statisíců. Cena se však nachází v limitu, kdy není potřeba vypisovat samotný investiční projekt. Veškeré náklady spojené se zavedením a certifikací pokryjí provozní výdaje. I když na první pohled vypadá, že je cena vysoká, při prvním vážnějším incidentu se tato investice navrátí. Velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře možných rizik. Všechny jmenované náležitosti však management společnosti zná z předchozího zavádění ISO 9001 (management kvality). Lze tedy předpokládat přehled v problematice po stránce časové i finanční.

Na základě provedené analýzy rizik se ukázalo, že nejdůležitější bude zavést opatření proti rizikům u aktiv jako je zdravotnická dokumentace (elektronická i listinná), informační a operační systém. Není možné opomenout také ochranu serveru a síťových prvků. Opatření pro tato aktiva jsem zanesla do bezpečnostní příručky a doplnila je dalšími návrhy na efektivní řízení bezpečnosti informací.

Zavedení opatření a certifikace dle ISO 27001 může přinést zefektivnění výdajů vkládaných do bezpečnosti. ISMS navíc zavádí ucelené a komplexní řízení bezpečnosti. Pomáhá rovněž splnit legislativní a právní požadavky. Nemalý přínos shledávám též v konkurenční výhodě a ve zvýšení důvěry ze strany pacientů a veřejnosti.

V rámci prováděné analýzy organizace se vedla diskuze o tom, zda by pan doktor certifikaci zvážil. Dle jeho slov již v minulosti o této variantě uvažoval. Nyní v souvislosti s novými zákony a nařízeními uvažuje o certifikaci v horizontu jednoho roku. Proto také

kladně reagoval, na můj dotaz ohledně možnosti aplikace diplomové práce na jeho zdravotnické zařízení.

# 7 Závěr

Ve své diplomové práci jsem se zabývala informační bezpečnostní ve zdravotnictví. Cílem bylo analyzovat konkrétní společnost a na základě zjištěných informací pro ni vytvořit bezpečnostní příručku.

Vybraná organizace se bezpečnostní doposud příliš nezabývala a nemá vypracované žádné konkrétní postupy, jak zabránit možným incidentům na vlastněná aktiva. Z důvodu citlivosti dat, které se v organizaci uchovávají a zpracovávají, by se mělo zvážit zavedení systému managementu bezpečnosti (ISMS). Pomocí mnou navržené bezpečnostní příručky se organizace může inspirovat a zhodnotit, jaká aktiva prioritně chránit. Navržená opatření má možnost zvážit při zavádění ISMS.

Zvýšení prestiže a další výhody lze očekávat po získání certifikátu dle ISO 27001, který by doplnil již získaný certifikát managementu kvality.

Hlavním přínosem této práce je její praktická využitelnost a možnost začlenit ji do systému organizace. Nyní již záleží pouze na vedoucím lékaři, zda návrhy na opatření vezme na vědomí a zavede je do provozu.

Domnívám se, že se cíle práce ve všech ohledech zcela naplnily.

# Bibliografie

1. **DOUCEK, Petr.** *Řízení bezpečnosti informací.* 2. rozšířené vydání o BCM. Praha : Professional Publishing, 2011. ISBN 978-80-7431-050-8.

2. **ONDRÁK, Viktor, SEDLÁK, Petr a MAZÁLEK, Vladimír.** *Problematika ISMS v manažerské informatice.* Brno : Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

3. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN ISO/IEC 27000:2014 Informační technologie - Bezpečnostní techniky - Systém řízení bezpečnosti informací - Přehled a slovník.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

4. **NOVÁK, Luděk a POŽÁR, Josef.** Systém řízení informační bezpečnosti. *CYBERSECURITY.* [Online] 2011. [Citace: 6. květen 2017.] http://www.cybersecurity.cz/data/SRIB.pdf. ISBN 978-80-7251-356-7.

5. **LOVEČEK, Tomáš.** *Bezpečnosť informačných systémov.* 1. vydání. Žilina : Žilinská univerzita v Žiline, 2007.

6. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* místo neznámé : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

7. **DOSEDĚL, Tomáš.** *Počítačová bezpečnost a ochrana dat.* Vydání první. Brno : Computer Press, 2004. ISBN 80-251-0106-1.

8. **POŽÁR, Josef.** *Informační bezpečnost.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

9. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN EN ISO/IEC 27799:2008 Zdravotnická informatika - Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2008.

10. **ISO.** International Organization for Standardization. [Online] [Citace: 17. Květen 2017.] www.iso.org.

11. **UNMZ.** Seznam ČSN. *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.* [Online] 2017. [Citace: 17. Květen 2017.] http://seznamcsn.unmz.cz.

12. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

13. **T-SOFT.** Co přináší zákon o kybernetické bezpečnosti. *TSOFT.* [Online] 2017. [Citace: 19. Květen 2017.] http://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/.

14. **Česká republika.** *Nařízení vlády č. 315/2014 Sb. o kritériích pro určení prvku kritické infrastruktury.*

15. —. *Nařízení vlády č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.*

16. **ŠKORNIČKOVÁ, Eva.** GDPR cirkus přijíždí. Začínáme! *Obecné nařízení o ochraně osobních údajů prakticky.* [Online] 27. Duben 2017. [Citace: 19. Květen 2017.] https://www.gdpr.cz/blog/gdpr-cirkus.

17. **ROOT.** eHealth v ČR: nová strategie bezpečné infrastruktury. *ROOT.CZ.* [Online] 24. Listopad 2016. [Citace: 19. Květen 2017.] https://www.root.cz/clanky/ehealth-v-cr-nova-strategie-bezpecne-infrastruktury/.

18. *Národní strategie elektronického zdravotnictví České republiky 2016-2020.* **NĚMEČEK, Petr.** Ročník 26, místo neznámé : Česká lékařská komora, Listopad 2016, TEMPUS MEDICORUM. ISSN 1214-7524.

19. **CSIRT.** Rozsáhlé útoky ransomwaru WannaCry . *CSIRT.* [Online] 15. Květen 2017. [Citace: 17. Květen 2017.] https://www.csirt.cz/page/3547/rozsahle-utoky-ransomwaru-wannacry/.

# Seznam obrázků

# Seznam tabulek